

TOP OFFICIALS (TOPOFF) EXERCISE SERIES

TOPOFF 2 (T2)

After Action Report

September 30, 2003



Homeland
Security



FOR OFFICIAL USE ONLY

This page intentionally left blank

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is *Top Officials (TOPOFF) Exercise Series: TOPOFF 2 (T2) After Action Summary Report*.
2. Information contained in this document is intended for the exclusive use of T2 Exercise Series participants. Material may not be reproduced, copied, or furnished to non-exercise personnel without written approval from the Exercise Directors.
3. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate Canadian, U.S. Department of Homeland Security (DHS), U.S. Department of State (DOS), the State of Illinois, the State of Washington, and local/city security directives. This document is marked For Official Use Only (FOUO), and information contained herein has not been given a security classification pursuant to the criteria of an Executive Order, but this document is to be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one or more FOUO exemptions.
4. Reproduction of this document, in whole or in part, without prior approval of DHS is prohibited.
5. DHS, Office for Domestic Preparedness (ODP), and DOS, the Office of the Coordinator for Counterterrorism, cosponsored the T2 Exercise Series. Mr. Theodore Macklin (b)(6) and Mr. Corey Gruber (202-514-0284) are the ODP Points of Contact (POC) and (b)(6) (b)(6), the Office of the Coordinator for Counterterrorism, is the POC for international play.
6. This report is intended for the use of Federal, State, and local (FSL) officials responsible for homeland security. It is intended to improve the FSL plans to prevent and respond to weapons of mass destruction by understanding the lessons learned from T2.

This page intentionally left blank

**Top Officials (TOPOFF)
Exercise Series:**

**TOPOFF 2 (T2)
After Action Summary Report**

**Prepared for
U.S. Department of Homeland Security
Office for Domestic Preparedness
by AMTI and the CNA Corporation
Under Schedule Number GS-10F-0324M,
Order Number 2003F028**

This page intentionally left blank

SUMMARY REPORT

I. Introduction

Top Officials (TOPOFF) 2 (T2) was a Congressionally-mandated, national combating terrorism exercise. The exercise was designed to improve the nation's domestic incident management capability by exercising the plans, policies, procedures, systems, and facilities of Federal, State, and local (FSL) response organizations against a series of integrated and geographically dispersed terrorist threats and acts.

T2 was cosponsored by the U.S. Department of Homeland Security (DHS) and the U.S. Department of State. The T2 After Action Report (AAR) provides the findings from the analysis of the Full-Scale Exercise (FSE), and also integrates the findings from the pre-FSE seminars and the Large-Scale Game (LSG).

The domestic objectives of the T2 exercise were to improve the nation's capacity to manage complex/extreme events; create broader operating frameworks of expert domestic incident management and other systems; validate FSL authorities, strategies, plans, policies, procedures, protocols, and synchronized capabilities; and build a sustainable, systematic exercise process for advancing domestic preparedness. There was also an international aspect of T2 that exercised a segment of the Canadian response to weapons of mass destruction (WMD) attacks upon the United States. This cross-border play focused on bilateral goals in the areas of communication, preparedness, and response to WMD terrorism incidents.

T2 was the largest and most comprehensive terrorism response exercise ever conducted within the United States. The T2 exercise scenario depicted a fictitious, foreign terrorist organization that detonated a simulated radiological dispersal device (RDD) in Seattle, Washington, and released the Pneumonic Plague (*Yersinia pestis*) in several Chicago area locations. There was also significant pre-exercise intelligence play, a cyber attack, and credible terrorism threats against other locations.

II. Background

A. T2 Authorization

Public Law 106-553 authorized T2, and Senate Report 106-404 outlined the concept. T2 supported the National Security Council's Policy Coordinating Committee on Counter-terrorism and National Preparedness Exercise Sub-group requirement for a large-scale, counterterrorism exercise commencing in 2002 and finishing in 2003. While T2 planning began under earlier Presidential Directives, the Homeland Security Presidential Directive (HSPD)-5 articulates the new federal incident management policy that ultimately guided the exercise. Participating FSL authorities were asked to submit exercise objectives to T2 planners at the start of the T2 design cycle to ensure that the exercise design would support participant objectives while also addressing national priorities.

B. Exercise Design and Concept

The first TOPOFF Exercise (TOPOFF2000) was a single, no-notice, FSE co-chaired by the Department of Justice and the Federal Emergency Management Agency (FEMA) in May 2000. Unlike TOPOFF2000, T2 was designed as an "open" exercise in which participants were introduced to the exercise scenario prior to the FSE through a cycle of exercise activity of increasing complexity that included:

- A series of seminars that explored emergency public information, RDD response, bioterrorism, and national direction and control issues;
- An LSG that explored intermediate and long-term recovery issues;
- An Advanced Distance Learning Exercise, conducted in conjunction with the *National Direction and Control Seminar*, that employed distance education technology to disseminate information and provide interactive training opportunities; and
- The *Top Officials Seminar* that brought together top government officials from 25 FSL agencies and departments, and the Canadian Government, in a round-table discussion to explore intergovernmental domestic incident management in response to WMD terrorist attacks upon the United States.

These activities culminated in an FSE which was played out from May 12 to May 16, 2003.

The purpose of the open exercise design was to enhance the learning and preparedness value of the exercise through a "building-block" approach, and to enable participants to develop and strengthen relationships in the national response community. Participants at all levels stated that this approach has been of enormous value to their domestic preparedness strategies.

III. Findings of the Exercise Analysis

A. Special Topics

The FSE exercised numerous critical aspects of the national response to radiological and bioterrorism attacks. This response cut across several predetermined areas of analysis, as decided by T2 participants in earlier exercise activities (see below). Specific special interest items included the following:

- Alerts and Alerting: The Elevation of the Homeland Security Advisory System Threat Level to Red;
- Declarations and Proclamations of Disaster and Emergency;
- Department of Homeland Security Play in T2: The Role of the Principal Federal Official;
- Data Collection and Coordination: Radiological Dispersal Device Plume Modeling and Deposition Assessment in Washington;
- Play Involving the Strategic National Stockpile;
- Hospital Play in the Illinois Venue: Resources, Communications, and Information Sharing during a Public Health Emergency;
- Decision-Making Under Conditions of Uncertainty: The Plague Outbreak in the Illinois Venue; and
- Balancing the Safety of First Responders and the Rescue of Victims.

B. Core Areas of Analysis

Rather than evaluating participant ability and performance or specific agency-by-agency objectives, the exercise evaluation methodology focused on the objective analysis of decision and coordination processes that support the nation's top officials and the broader system of FSL agencies. The exercise events were analyzed as they unfolded in light of six major areas of analysis, identified through a survey of TOPOFF 2000 findings, and other exercise or real-world lessons learned:

- Emergency Decision-Making and Public Policy;
- Emergency Public Information;
- Communications, Coordination, and Connectivity;
- Jurisdiction;
- Resource Allocation; and
- Anticipating the Enemy.

IV. Artificialities

Artificialities are inherent in every exercise and result from the simulated nature of exercises. False conclusions can arise if the natures and effects of artificialities are not accounted for during the analysis process. Some artificialities were essential in exercise design including the simulated RDD explosion, prescheduled top official play, limited public involvement, and notional road closures. Some artificialities were specific to the T2 design process, such as the known scenario and the lack of 24-hour play by some entities. Other T2 artificialities, while not preplanned, were nonetheless anticipated in the exercise, as it encouraged free play. The evaluation team researched, documented, and factored all such artificialities into the analysis of the FSE.

V. Special Topics

A. Alerts and Alerting: The Elevation of the Homeland Security Advisory System Threat Level to Red

The FSE exercised the use of the Homeland Security Advisory System (HSAS); the decision to elevate the HSAS Threat Level to Red; and the actions associated with Threat Level “Severe,” or Red. It also allowed examination of the implications of raising specific regions or localities to Red. The FSE highlighted that further refinement of this advisory system is needed.

Significant findings from the FSE include the following:

- Following the local threat level elevations of Seattle and King County early in the FSE, there was uncertainty as to the status of the HSAS Threat Condition of other jurisdictions. This situation was caused in part by a) a lack of awareness of local threat advisory systems; b) inconsistent or nonexistent formal notification protocols of threat elevations; and c) a lack of language clarity—elevations of the HSAS are referred to as elevations of the “National Threat Level,” even if applied to regions or localities;
- The FSL response to elevations of the HSAS needs to be further developed and synchronized. Participants in the T2 After Action Conference (AAC) suggested the development of a tiered, operational response linked to the HSAS levels and based upon the nature of the threat. This system would be defined by a coalition of FSL agencies and would offer a comprehensive operational response framework that jurisdictions at all levels could use to help define their response plans at each HSAS Threat Condition. DHS is leading an interagency effort to review these recommendations and make appropriate refinements to the HSAS; State, local, and private sector constituents are active partners in this process; and
- Agencies are concerned about the lack of specific intelligence accompanying threat level elevations and the cost of maintaining a raised threat level. DHS is currently examining ways to improve information flow to and from State and local governments and the private sector regarding changes in alert level. Also, the DHS-led HSAS Working Group is currently addressing the economic and operational impacts of a raised threat condition.

B. Declarations and Proclamations of Disaster and Emergency

During the FSE, several declarations and proclamations of emergencies and disasters were issued. Local and State jurisdictions in both exercise venues invoked their authorities to declare emergencies and requested Federal assistance under the Stafford Act. These requests ultimately led to a Presidential Declaration of Major Disaster in Washington and a Presidential Declaration of Emergency in Illinois. The bioterrorism attack in Illinois was especially challenging as its impact involved multiple counties, the city of Chicago, and the state of Illinois. In addition, the Secretary of the Department of Health and Human Services (HHS) declared a Public Health Emergency in the state of Illinois under the authorities of the Public Health Service Act. This occurred before the Presidential Declaration of Emergency, enabling the activation of several response assets.

Significant findings from the FSE include the following:

- Officials in Illinois requested a Major Disaster Declaration to obtain maximum Federal assistance for the growing bioterrorism disaster, out of concern for the perceived five million dollar limit and other limits to Federal assistance in declarations of emergency. Some were unaware that the President can approve an expenditure of funds in excess of that limit under the conditions where, as stated in the Stafford Act, “continued emergency assistance is immediately required; there is a continuing and immediate risk to lives, property, public health, or safety; and necessary assistance will not otherwise be provided on a timely basis.” In addition, the nature of the declaration in Illinois led to concerns about whether some individual assistance programs, which are specifically authorized for a disaster but not for an emergency, would be authorized;
- It is worth noting that during the FSE, the President did not declare the large-scale bioterrorism attack a Major Disaster under the Stafford Act. It is not clear from the FSE whether the difference in declaring an emergency or a major disaster would result in substantive operational issues given the exception clauses under declarations of emergency as previously described;
- There was some uncertainty regarding the relationships between State and local declarations of emergency. In Illinois there was some uncertainty as to whether county-level declarations needed to be enacted in light of a State declaration of emergency or whether a state declaration made these moot. Officials determined that in legal terms, county-level declarations needed to be enacted, even when preceded by a State declaration of emergency, to access funds that the State declaration made available; and
- The relationships between the authorities and resources brought to bear under the Public Health Act and the Stafford Act should continue to be exercised. Additional clarity regarding the authorities and resources brought to bear under both Acts is required.

C. Department of Homeland Security Play in T2: The Role of the Principal Federal Official

The FSE was the first major opportunity for the newly created DHS to exercise and experiment with its domestic incident management organization, functions, and assets. For example, the DHS Principal Federal Official (PFO) concept was first implemented during the FSE, which provided the opportunity to examine the role of the PFO during an emergency response. During the FSE, the PFOs in both venues facilitated integrated communications and coordinated action planning. In addition, they both encouraged active communications with state and local authorities.

Significant findings from the FSE include the following:

- The PFO was well-received and successfully integrated into the unified command structure in both venues. In Seattle, the PFO quickly instituted a unified command to manage the overall Federal response and coordinate integrated communications and action planning. The PFO in Seattle also helped to prioritize and adjudicate between the often-competing needs of the crisis and consequence management sides of the response phase. In Illinois, the PFO worked within the framework of a unified command to ensure that integrated communications were achieved and that action plans were coordinated;

- The PFO relationships with Federal officials differed in part due to the different problems that each encountered with the two different attacks. In Seattle, although an RDD was involved, the event unfolded in more of a traditional first-responder fashion with a relatively well-delineated disaster site. In Illinois, events unfolded more gradually, as would be expected in a disease outbreak. As a result, the PFOs in each venue had different relationships with the FEMA Regional Director (RD), the FEMA Federal Coordinating Officer (FCO), and the FBI Special-Agent-In-Charge (SAC). The roles and responsibilities of the PFO relative to FEMA and FBI officials have been clarified through issuance of the Initial National Response Plan (INRP); and
- Both PFOs required additional technical support beyond their deployed administrative and security details. The FSE highlighted the need for the PFO to have a dedicated staff with the flexibility and expertise to support all emergencies, natural and terrorist-related. DHS has recently developed operational procedures for providing additional resources to the PFO to facilitate domestic incident management activities. Further delineation of the roles and responsibilities of the PFO, as well as PFO support requirements, will be included in the final version of the National Response Plan (NRP).

D. Data Collection and Coordination: Radiological Dispersal Device Plume Modeling and Deposition Assessment in Washington

During the FSE, there were multiple FSL agencies that had responsibilities for collecting data. The data was then sent to one or more locations to be compiled and analyzed. Once the analyses were complete, information was provided to top officials to assist in their decision-making. However, there were critical data collection and coordination challenges that impacted the response to the RDD attack in Seattle, to include the provision of timely, consistent, and valid information to top officials.

Significant findings from the FSE include the following:

- The coordination of onsite and offsite data collection by multiple agencies at FSL levels of government needs to be improved. The FSE highlighted the many radiological data collection assets that exist at all levels of government. FSL agencies and departments, therefore, need to be educated about the importance of coordinating the data collection process, and to work with the Federal Radiological Monitoring and Assessment Center (FRMAC) to ensure that coordination takes place during radiological emergencies. The development of the NRP will more clearly delineate the data collection and coordination processes in the future;
- The development and distribution of multiple radiological plume analysis products—including plume model prediction overlays and empirical deposition/footprint maps—to decision-makers needs to be better coordinated. Different FSL agencies and jurisdictions used one or more plume models to generate predictions. Each jurisdiction also developed its own data products based upon separate and sometimes conflicting empirical data. As a result, Seattle, King County, and Washington State top officials had different or conflicting information upon which to base their decisions. In addition, several Federal agency and department headquarters developed their own plume predictions to make internal assessments concerning assets that might be required. Conflicting predictions were, therefore, presented to department and agency top officials;

- There is a need for additional education among both responders and decision-makers as to the timing and value of the different types of information following a radiological incident. The value and limitations of plume models and other analysis products are not widely understood. Importantly, it appears as though few decision-makers were informed of the limited usefulness and lifecycle of plume models. Plume models provide a prediction of where the material in the explosion will travel. They can be useful in assisting decision-makers in making preliminary decisions regarding likely areas of contamination. Once actual data from the incident is collected and evaluated, the value of plume models diminishes. Once responders learn what really is out there and where it is, predictions alone become less important. However, predictions updated with initial measurement data can be useful in estimating protective actions in areas that have not yet been surveyed, or in areas that have been contaminated below the measurement threshold of available instruments; and
- The Homeland Security Council is leading an interagency effort to remedy the plume modeling process deficiencies noted during the exercise.

E. Play Involving the Strategic National Stockpile

The activation, requests for, deployment and distribution of the Strategic National Stockpile (SNS) were extensively played during the FSE. The exercise tested the ability of all levels of government to make decisions, allocate resources, coordinate and communicate, and inform the public regarding this critical SNS resource. The state of Illinois tested its ability to break down and secure the antibiotic stocks, and local jurisdictions tested their abilities to distribute supplies of antibiotics to their first responders and citizens. Overall, the request, receipt, breakdown, distribution, and dispensing of the SNS during the FSE were completed successfully. Some components of the SNS were not tested during the exercise. Some aspects of the requesting process exercised in T2 presented specific challenges.

Significant findings from the FSE include the following:

- Determining a prophylaxis distribution policy for first responders and citizenry across local jurisdictions was challenging. This was due, in part, to the enormous logistical challenges of distributing medications to a large metropolitan area, as well as the very real limitation of the amount of medication that was immediately available. Determining a prophylaxis distribution policy was also challenging due to the need to factor in anticipated public reaction if the general citizenry were not given access to the medication;
- Contradictory information complicated decision-making with respect to the allocation of the SNS. Decision-makers experienced difficulty determining the amounts in local stockpiles; how much the State had and how its amount would be allocated; and how much would be coming from the SNS, when it would arrive, and how much each jurisdiction would receive;
- Inconsistent information was given by different jurisdictions as to who should seek prophylaxis and when, the locations of the suspected plague release sites, and whether one should stay home or seek medical attention; and

- The Homeland Security Council is leading an interagency working group to resolve the mass prophylaxis issues that arose during the exercise.

F. Hospital Play in the Illinois Venue: Resources, Communications, and Information Sharing during a Public Health Emergency

During the FSE, 64 hospitals in the Illinois venue participated in the exercise, making it one of the largest mass casualty exercises ever undertaken. This aspect of T2 presented an unprecedented opportunity to examine the coordinated efforts of the medical and public health communities to react to and control the spread of a disease outbreak, specifically an outbreak initiated by a bioterrorism attack. Because of the large number of participating hospitals, challenges regarding communication and the management of resource requirements were significant.

Significant findings from the FSE include the following:

- During the FSE, the lack of a robust and efficient local emergency communications infrastructure was apparent. Communications heavily relied upon telephones and faxes for data transmission. The unanticipated large call volume was the greatest problem. The phone system in at least one location was overwhelmed, requiring three amateur radio operators to maintain communications connectivity. Facsimile communications were also subject to transmission and receipt problems due to call volumes. “Blast fax transmissions” took up to two hours to complete. In addition, information was often copied manually to a form. The form was then faxed (in some cases degrading its readability) to a collection point, where it was then manually tabulated on another form, and then entered into an information system for transmission. This process significantly increases potential errors; and
- Resource demands challenged hospitals throughout the FSE. These included short supplies of isolation and negative pressure rooms, as well as staff and bed shortages. Hospitals employed a number of solutions to these problems including activating staff phone trees to recall medical personnel; using extra conference rooms, lobbies, and Clinical Decision Units (closed units) as isolation wards; and using same-day surgery, radiology, and endoscopy labs, as well as an offsite tent, as negative pressure (i.e., disease containment) rooms.

G. Decision-Making Under Conditions of Uncertainty: The Plague Outbreak in the Illinois Venue

During a disease outbreak, whether naturally occurring or initiated by an act of terrorism, decision-makers must make effective response decisions. Officials rely upon scientists, medical doctors, and the public health system to provide them with the best scientific information. It is this information that decision-makers must use to formulate answers within the context of the logistical, political, social, public health, and economic aspects of a response. This is especially difficult following terrorist attacks due to the enormous media and time pressures that decision-makers will operate under. During the FSE, public health officials initially were uncertain as to the extent and possible duration of the plague epidemic. This produced an environment where officials had to make decisions without the benefit of positive-proof information.

Significant findings from the FSE include the following:

- Coordination processes between agencies and across jurisdictions regarding epidemiological model predictions and patient data need to be improved. In fact, information about some modeling efforts was not provided to all operations centers during the FSE;
- There needs to be an enhanced understanding of the implications of long-term patient load during a bioterrorism incident. Two issues of concern are: (1) a lack of confidence in the patient data, and no clear way to model the long-term effects in the face of poor patient data; and (2) a lack of long-term exercise play—the FSE concluded before the extensive scale of the outbreak was apparent;
- During the early stages of an outbreak, decision-makers are likely to see reports about only the early presenters, not the full number of exposed persons. It is absolutely critical to determine rapidly the scale of the outbreak. This is especially true in cases of potential bioterrorism where traditional epidemiological curves could be multiplied by multiple, continuing, or widespread initial exposures; and
- The Homeland Security Council is leading an interagency effort to resolve mass care and medical surge capacity issues that arose during the exercise.

H. Balancing the Safety of First Responders and the Rescue of Victims

During incidents when victim survival is dependent upon the timeliness of medical treatment, first responders typically initiate victim rescue and removal as rapidly as possible, while incident commanders manage responder safety with an ongoing risk-benefit analysis. However, when faced with an emergency that potentially involves WMD, first responders face a greater potential of becoming casualties themselves. Given the uncertainty surrounding the simulated RDD explosion during the FSE, even when many of the responders artificially had the knowledge that it was a radiological incident, the incident commander had to take precautions to ensure that the responders were safe. However, a number of public health officials and data collectors at the incident site, many of whom were subject matter experts, expressed concern about the time it took to triage, treat, and transport victims.

Significant findings from the FSE include the following:

- Rescue operations at the RDD incident site highlighted the need for more frequent, informational communication between incident command and hospital control. Incident commanders may need to be more proactive in providing information. While hospital control was aware that radiation had been detected at the incident site, there is no indication in the data analyzed that incident command or the medical group at the incident site communicated with hospital control to explain the need to conduct a more detailed risk-benefit analysis before rescue operations could commence. In addition, hospital control was unaware of the periodic halts to rescue operations that occurred during the initial hours of the exercise response due to both the suspected and simulated presence of secondary explosive devices; and
- The public health and medical communities, the media, and the general public should be educated on the unique considerations that must be factored into rescue operations following a terrorist WMD attack. Considerations non-responder communities should be aware of are the need to balance responder safety and rescue efforts and the specific

practices rescuers employ when responding to critical situations, such as the potential for secondary explosive devices in or around an incident scene. The public health and medical communities should be made aware of the need for incident command to conduct a detailed risk-benefit analysis prior to the start of rescue operations. Finally, a consistent message to the public from incident command, public health, and medical communities is critical.

VI. Six Core Areas of Analysis

A. Emergency Public Policy and Decision-Making

Emergency Public Policy and Decision-Making encompasses the unique challenges, difficulties, and nuances faced by top officials in the initial aftermath of a terrorist WMD attack. During the FSE, top officials were faced with two critical decisions that have not yet occurred in the real world: (1) elevations of the threat status to Red by City, County, and Federal authorities; and (2) a request for and issuance of Presidential Declarations for RDD and bioterrorism attacks.

Significant findings from the FSE include the following:

- Making decisions under conditions of uncertainty, when information is rapidly changing or unknown, remains a significant challenge. Decision-makers experienced challenges obtaining reliable, validated, and timely information. In the case of bioterrorism, the parameters are difficult to define, and the full extent of the effects from such an attack may be unknown. During a physical disaster, such as the case of an RDD blast, the parameters can often be roughly determined, but life-saving and public safety decisions may be required before perfect information is available;
- Greater understanding is needed of the mid- to long-term impacts of multiple terrorist attacks. The FSE did not play out long enough for participants to face the long-term economic, health, social, or political implications of the scenario. To more thoroughly examine long-term issues, the private sector should be encouraged to participate more extensively in future TOPOFF exercises and events; and
- The international aspect of T2 and the active participation of the Canadian Government represented a significant new element of the TOPOFF Exercise design. The cross-border play expanded the scope of decisions faced by domestic top officials during the FSE and enhanced the realism of the exercise.

B. Emergency Public Information

Emergency Public Information encompasses the unique public information challenges and implications faced by top officials and their support staff in the midst of a terrorist WMD attack. Emergency public information was a dominant issue of TOPOFF 2000 and remained one throughout the T2 seminars, LSG, and FSE. T2 provided a unique opportunity for jurisdictions at all levels to exercise, experiment with, and improve upon critical public information strategies. This exercise was an opportunity for participants to showcase the value of concepts, such as regional Joint Information Centers (JICs), that may be expanded for more comprehensive coordination at both broader FSL levels and in environments where people cannot be physically co-located.

Participants commented that future TOPOFF Exercises should continue to allow participants to experiment in the emergency public information arena, which should include an aggressive news-gathering element and a realistic mock-public response to further challenge exercise participants.

Significant findings from the FSE include the following:

- Speaking with one voice proved to be one of the greatest emergency public information challenges during the FSE. JICs were implemented in both venues and helped to unify messages, but not all information was coordinated through the JICs. In both venues, however, the DHS PFO emphasized and worked for a consistent Federal message that was also consistent with the State and local messages;
- Official messages to the public regarding protective action guidelines were often incomprehensive or conflictive;
- Rumors abounded during the FSE. Determining which statements were true proved to be a significant challenge for T2 participants. Improving official channels of communication would help to counter and confirm rumors. Ensuring accurate information depends upon having structured, well-defined, and robust information flow strategies, where information is accepted from predefined validated sources. Such strategies exist in numerous policies such as the INRP, but implementation of them remains a challenge. Although the exercise did not play out long enough in either venue to establish how the long-term role of the PFO might affect information flow, during a disaster, the PFO role has the potential to strengthen and streamline the movement of key information between the State and local governments and Federal agencies;
- Even though the need for pre-coordinated information packages was mentioned throughout the seminars and during the LSG, many agencies lacked a full set of pre-coordinated, off-the-shelf packages prior to the FSE; and
- DHS has led an interagency effort to successfully remedy the incident communications deficiencies noted during TOPOFF 2000. Results include an interagency-approved incident communications strategy, hotline, subject matter expert reach-back, and improved FSL incident communications processes and protocols.

C. Communications, Coordination, and Connectivity

Communications, Coordination, and Connectivity encompasses the challenges that result from information exchange across all levels of government, the information flow that supports decision-makers, and the electronic means by which information is shared. Communications, coordination, and connectivity issues probably present the greatest challenges when responding to a mass casualty incident, especially one involving WMD. During the FSE, several challenges emerged in these three dimensions of information exchange. A lack of coordination was the primary communication challenge observed during the FSE.

Significant findings from the FSE include the following:

- There were numerous instances when participants experienced difficulties obtaining or validating information. In the absence of a commonly understood process for official notifications, agencies had difficulty confirming the status of the HSAS Threat Level for

several hours. Also, agencies spent substantial time confronting rumors regarding, among other misinformation, transportation closures, patient numbers in both venues, and casualty figures at the RDD scene. Some agencies attributed these problems to too many official reporting channels, where various agencies exercised not only their own independent procedures but also redundantly requested updates from agencies;

- Inconsistent language was another communication challenge during the FSE. In Washington State, confusion arose as many participants interchangeably used the term *casualties* to mean *fatalities* or *injured people*, or both. Similarly, the nonspecific references to plague in internal agency communications resulted in at least one instance when a public health person gave advice that applied to Bubonic Plague rather than Pneumonic Plague;
- Officials also remarked on the critical importance of having technical data translated into non-technical language to support decision-making and risk communications;
- Data collection and coordination issues challenged both the Washington and Illinois venues. In Washington, the primary coordination challenges involved the collection and reporting of radiological ground data and the apparent lack of a unified command structure during the early stages of the response at the RDD site. In Illinois, the greatest coordination challenges involved the collection of information and the data flow requirements among the 64 hospitals, the five POD hospitals (the five lead hospitals for coordinating disaster medical response in a specific region upon activation of the emergency medical disaster plan by Illinois Operations Headquarters and Notifications Office (IOHNO)), and three separate but interrelated statewide organizations: Illinois Department of Public Health (IDPH), IOHNO, and the Illinois State Emergency Operations Center (EOC);
- The FSE provided opportunities for participation from some organizations not typically included in a response, and also encouraged some organizations to participate in new ways. For example, the American Red Cross participated in the Federal Joint Operations Center (JOC) and Bank of America co-located an EOC with the Federal Reserve. Further, participants reported that the T2 building-block process was extremely valuable in helping them to develop new or stronger relationships with their colleagues at all levels; and
- Connectivity challenges impacted the ability of technical experts, agencies, and jurisdictions to communicate effectively. Hospitals and the medical system lack robust Internet-based communications systems in many cases and overwhelmingly rely on phones and faxes for transmitting and tracking critical patient and resource information which is extremely inefficient. In Illinois, organizations reported their fax machines were unreliable due to mechanical breakdowns and an inadequate number of staff to monitor them. Also some machines were reported to be in locked rooms. Likewise, the lack of verified phone numbers caused communication delays while emergency personnel spent critical time looking for the correct numbers to report emergency data. In Washington, the Department of Health Radiation Monitoring and Assessment Center (RMAC) and FRMAC experienced significant connectivity challenges that impacted their ability to distribute data and data products, respectively, to decision-makers, subject matter experts, and responders.

D. Jurisdiction

Jurisdiction encompasses the issues, conflicts, or gaps in authorities and the assumptions that may arise when policies and agreements are put into practice under the uniquely challenging conditions of a terrorist WMD attack. The FSE demonstrated that jurisdictional policies and the extent to which they are understood by various entities drive and influence every element of response. Participants at all levels of government continue to state that exercises such as TOPOFF remain one of the most effective means to explore the operational implications of these jurisdictional policies and refine authorities that may appear clear on paper but which lack clarity when implemented under the complex conditions of a disaster.

Significant findings from the FSE include the following:

- Throughout the T2 cycle, the primary jurisdictional question evolved from “who is in charge” to “who is in charge of what.” During the FSE, there was some confusion with the multiple, and sometimes overlapping, authorities that were driving the disaster response. For example, in Illinois there were many discussions concerning the jurisdiction over the decontamination process and the facilities where the biological agent was released (the United Center, O’Hare International Airport, and Union Station). Similar questions arose in the Washington venue regarding the management of the long-term impacts of the radiological contamination;
- The FSE provided an opportunity to explore jurisdictional issues involving DHS. For example, there was uncertainty between the Transportation Security Administration and the Federal Aviation Administration regarding the authority to close and reopen airspace and issue temporary flight restrictions. Issues also arose regarding the activation, requests for, deployment, and distribution of the SNS, where both HHS and DHS are involved in these processes. Furthermore, questions arose regarding the relationship between HHS and DHS during a Public Health Emergency, and how expertise and health and medical assets—which are now split between DHS and HHS—are used and managed. The FSE helped to highlight areas where the role of the PFO as it relates to FEMA officials needs additional clarification. Lastly, the Environmental Protection Agency noted the need to clarify its authorities relative to DHS, specifically noting development and maintenance of health and safety plans; and
- The authority to release information can be especially problematic when a disaster crosses jurisdictional boundaries, as was the case during the FSE with both the RDD and bioterrorism attacks. Organizations at State and local levels repeatedly expressed concerns about Federal organizations releasing information that the State and local organizations believed they should have released instead.

E. Resource Allocation

Resource Allocation encompasses the challenges that require decision-makers to weigh conflicting needs and determine how best to allocate limited resources. Conflicting resource needs can challenge decision-makers within a single agency, or can force decision-makers from different agencies and departments to work together under stressful and time-constrained conditions to decide how best to manage critical resources that are in short supply. Often the solution requires individuals and organizations to use unconventional methods.

While the scenario did not fully stress the Washington venue resources and the FSE ended before the number of plague patients overwhelmed the Chicago area medical and public health capabilities, a number of resource allocation issues and “best practices” emerged.

Significant findings from the FSE include the following:

- State and local participants were often not aware of which Federal resources were available and how to access them. State and local emergency managers and responders would benefit from an “Emergency Response Knowledge Base,” or Procedural Flow, that described all Federal assets, helped State and local officials identify those assets that would best meet their needs in an emergency, and explained how to request the response assets;
- A “one stop shop” for tracking the status of Federal assets that have been activated or deployed during an emergency does not exist. FEMA currently tracks and reports the usage of Federal assets in a disaster through its Mission Assignments and Situation Reports, but distribution of these reports is fairly inefficient. A Web-based, searchable knowledge base of all available Federal resources and their status (potentially expanded to include State and local resources) may be helpful in this regard, particularly when resources are stressed;
- Having a contingency plan for the receipt and distribution of the SNS contributed to a fairly smooth-running process in Illinois. In contrast, shipment and distribution of the National Pharmaceutical Stockpile (the previous name for the SNS) did not transition as smoothly in the TOPOFF 2000 exercise. In part, this reflects the tremendous investments in planning and preparedness that have occurred in State and local public health departments since the fall of 2001;
- Participants utilized unconventional strategies to meet resource demands. They did this by relying on unconventional sources of support and by intervening with executive orders that exempt individuals from repercussions that were often legal and which would otherwise prevent them from providing services; and
- Decision-makers anticipated future demand. In Washington, several assets were placed on standby in case they were needed at another incident site. Illinois emergency managers and public health officials developed a plan to deal with the limited supply of medication and anticipated potential hospital surge requirements that the growing epidemic would require. In Washington, D.C., the DHS Emergency Preparedness and Response Directorate worked on a plan to distribute the SNS to other states that requested it, recognizing the inevitable spread of Pneumonic Plague cases outside Illinois.

F. Anticipating the Enemy

Anticipating the Enemy encompasses the unique considerations that influence decision-making when there is a potential enemy threat. The existence of an enemy makes the response to a terrorist attack qualitatively different from the response to any natural or conventional disaster. For example, the desire to keep the terrorists from gathering information regarding response plans works against the desire to keep the public informed.

Significant findings from the FSE include the following:

- There were a number of responder and top official activities that demonstrated a keen awareness of potential follow-on attacks. In Washington, the National Guard Civil Support Team was released from the incident site in part so that they would be available to redeploy in the event of another terrorist attack. In the Chicago area, authorities increased surveillance and decreased parking and deliveries at likely terrorist targets after the RDD explosion in Seattle. At the interagency venue, HHS, DHS, the Centers for Disease Control and Prevention, and others gave considerable thought to the need to reserve the SNS and other resources, specifically mentioning that Chicago might not be the only city to have been attacked with Pneumonic Plague;
- Many agencies stated that they either were not playing against an enemy or that it was the responsibility of others (e.g., the Federal Bureau of Investigation (FBI) and the JOC) to consider the enemy. However, when participating in a response, agencies should be aware that their responders are at risk. The loss of responders in additional attacks could seriously impair an agency's response capability, not to mention how such a loss would impact the morale of other responders and the public at large; and
- While an active opposing force, known as a Red Team, was limited in scope during the FSE, even its limited presence was beneficial to employing a more robust Red Team in future exercises.

VII. Exercise Design and Conduct Lessons Learned

The T2 AAC attendees and exercise participants identified several lessons learned relating to exercise design and conduct. Considerations for developing the following areas may benefit the success of succeeding TOPOFF Exercises: 1) planning and participation, 2) exercise artificiality, 3) scenario scripting, 4) the role the Virtual News Network (VNN), 5) a functional Web-based control capability, and 6) exercise security.

Other considerations worth investigating are the intelligence development and management processes, the guidelines for producing and publishing exercise documents, the standards for determining official exercise time, and methods for empowering the venue design and coordination teams.

VIII. Conclusions

T2 was an innovative, useful, and successful exercise built upon the accomplishments of TOPOFF 2000 and was the first national combating terrorism exercise conducted since DHS was established. As a result, T2 provided a tremendous learning experience for both the new DHS and the Federal agencies now working with DHS during a response to domestic incidents. In addition, the experience in Washington and Illinois provided important lessons regarding FSL integration. These lessons are valuable to other states and localities as they work to train, exercise, and improve their own response capabilities.

T2 involved the play of new agencies and entities within DHS (e.g., the Transportation Security Agency, the PFO, and the Crisis Action Team).

- The PFO concept was tested in both exercise venues. While this position has the potential to assist greatly with the coordination of Federal activities across the spectrum

of the response, T2 results also indicated that the roles and responsibilities of the PFO need to be clarified with respect to those of the FBI SAC, the FEMA RD, and the FCO. In addition, the PFO requires an emergency support team with the flexibility and expertise to provide support across the full range of homeland security operations.

T2 represented the first time (real or notional) in which the HSAS Threat Level was raised to Red.

- Valuable experience was gained as the Secretary of DHS, in concert with the Homeland Security Council, first raised selected areas of the country and then the whole country to Threat Level Red. In addition, local jurisdictions raised their own threat levels to Red.

T2 involved an extraordinary sequence of two Presidential Declarations wrapped around a Public Health Emergency declaration by the Secretary of HHS.

- The Presidential declarations were for a major disaster in the Washington venue and an emergency in the Illinois venue. These two declarations illustrated some of the subtleties of the Stafford Act that may not have been fully appreciated before the exercise; for instance, a bioterrorism attack does not clearly fit the existing definition of *disaster* as defined by the Act. The Secretary of HHS, acting on authorities through the Public Health Service Act and in consultation with the region, declared a Public Health Emergency. This permitted HHS to authorize the use of Federal assets (with costs covered by HHS).

Planning and development of the NRP and National Incident Management System should take advantage of the TOPOFF Exercise Series.

- Communication and coordination issues drove the course and outcome of critical public policy decisions, from raising the threat level to the various disaster/emergency declarations, and from the determination of exclusion zones to the reopening of transportation systems. To the extent that there were problems in these areas, communication issues were likely the primary cause; and
- T2 showed that how people believe communications and coordination should work as based upon policy is often not how they work in reality. What may appear to be clearly defined processes—such as requesting the SNS—in practice become much more difficult.

With the active participation of 64 hospitals in the Chicago area responding to the notional bioterrorism attack, T2 represented one of the largest hospital mass casualty exercises ever conducted.

- T2 represented a significant experiment in communications and coordination for the public health and medical communities. In particular, the massive amounts of communication required to track resource status (beds, specialized spaces, and medical equipment), and the cumbersome procedures and insufficient electronic means to do so in many cases, taxed hospital staff;
- T2 did not allow full exploration of the impacts of mass casualties on the medical system. Much less than half of the infected population was visible to the medical system at the conclusion of the exercise; and

- While there were a number of attempts to estimate the potential scope of the outbreak, the focus of most activities appeared to be on the cases that were presented to the health care system. It should be noted that HHS was working actively during the FSE to identify the resources that would be required to deal with the infected population.

T2 Illinois play also involved an extensive SNS request and distribution component.

- Although the actual distribution process appeared to go quite well, there was some confusion over the procedures and processes for requesting and receiving the SNS. The SNS Operations Center coordinated the stockpile deployment through the FEMA Emergency Preparedness and Response Director. Additionally, senior-level consultation occurred between DHS and HHS via Video Teleconference and direct communication; and
- The jurisdictions in the Chicago area were forced to confront important decisions about how the stockpile (and local assets) would be divided and who would be among the first population groups to receive prophylaxis. The discussions and decision-making involved, as well as the challenges in coordinating public information, are worthy of study by other metropolitan areas for the lessons they provide.

DHS should consider the integration of existing response policies and plans into the NRP.

- States are familiar with and have built their response plans to coincide with Federal assets and plans using similar agency and department structures and language;
- Federal agencies are satisfied with the language, authorities, and relationships outlined in existing plans such as the Federal Radiological Emergency Response Plan and the Federal Response Plan; and
- As the NRP undergoes development, the integration of response plans and policies merit consideration—particularly where existing plans are considered effective for emergency response.

T2 involved more intense and sustained top officials play than occurred during TOPOFF 2000.

- Of particular note was the involvement of DHS (which had been in existence for only a little more than ten weeks prior to the exercise), the DHS Secretary, and other senior civilians;
- HHS operated the Secretary's Command Center for 24 hours per day throughout the exercise with extensive play at the Assistant Secretary- and Operating Division Director-levels. The Secretary was actively involved, and since one venue involved substantial public health and medical play, the active participation of HHS was critical to the success of the exercise; and
- In both Washington and Illinois, the offices of the mayors, county executives, and governors were well-represented throughout the exercise by either the elected officials themselves or high-level policy-makers in respective administrations. In particular, the Mayor of Seattle participated substantially in the FSE, providing local top leadership that greatly contributed to the realism of play and to a greater appreciation of the local challenges and perspectives in a national WMD incident.

T2 represents a foundational experience to guide the future development of the TOPOFF Exercise Series.

- Because of the extensive data collection process and the effort to make T2 findings both well-documented and traceable through a detailed reconstruction of the exercise events, T2 represents a baseline upon which subsequent TOPOFF exercises can build and to which they can be rigorously compared;
- T2 demonstrated the value of the international, private sector, and nonprofit perspectives and roles in response to WMD terrorism. Future exercises will, no doubt, expand upon these elements by broadening the participation of all these sectors;
- Red Team activities during T2 provided ground rules for the involvement of a simulated active enemy threat in future exercises. This play should also be expanded in future exercises, as it represents one of the fundamentally different challenges responders face in a terrorist WMD disaster relative to any natural or conventional disaster; and
- The success of the VNN and widespread participant feedback regarding the desire for additional challenges in the area of public information suggest that future exercises should include a more aggressive mock-media element with a more aggressive news-gathering function that includes mock-press conferences.

This page intentionally left blank

PARTICIPATING AGENCIES LIST

United States Federal Departments and Agencies
American Red Cross (ARC)
Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)
Centers for Disease Control and Prevention (CDC)
Defense Threat Reduction Agency (DTRA)
Department of Agriculture (USDA)
Department of Defense (DoD)
Department of Energy (DOE)
Department of Health and Human Services (HHS)
Department of Homeland Security (DHS)
Department of Housing and Urban Development (HUD)
Department of Justice (DOJ)
Department of Labor (DOL)
Department of Navy (DON)
Department of the Interior (DOI)
Department of State (DOS)
Department of Transportation (DOT)
Department of Veterans Affairs (VA)
Environmental Protection Agency (EPA)
Federal Bureau of Investigation (FBI) – Critical Incident Response Group (CIRG)
FBI – WMD Countermeasures Unit
Federal Aviation Administration (FAA)
Federal Emergency Management Agency (FEMA)
General Services Administration (GSA)
Institute for Security Technology Studies (ISTS)
Joint Forces Command (JFCOM)
National Aeronautics and Space Administration (NASA)
National Imagery and Mapping Agency (NIMA)
National Reconnaissance Office (NRO)
National Security Council (NSC)
National Weather Service (NWS) (Department of Commerce)
Nuclear Regulatory Commission (NRC)
Occupational Safety and Health Administration (OSHA)

United States Federal Agencies and Organizations (Continued)	
Postal Inspection Service (U.S. Postal Service [USPS])	
Small Business Administration (SBA)	
Social Security Administration (SSA)	
Technical Support Working Group (TSWG)	
Transportation Security Administration (TSA)	
U.S. Coast Guard (USCG)	
U.S. Customs Service (USCS)	
U.S. Geological Survey (USGS)	
U.S. Secret Service (USSS)	
Canadian Agencies	
Agriculture and Agri-Food Canada (AAFC)	
British Columbia Ministry of Health EOC (BCMOH)	
British Columbia Provincial Emergency Program (BCPEP)	
Canadian Coast Guard (CCG)	
Canada Customs and Revenue Agency (CCRA)	
Canadian Food Inspection Agency (CFIA)	
Canadian Nuclear Safety Commission (CNSC)	
Canadian Security Intelligence Service (CSIS)	
Citizenship and Immigration Canada (CIC)	
Department of Justice (DOJ)	
Department of Defense (DoD)	
Department of Foreign Affairs and International Trade (DFAIT)	
Environment Canada (EC)	
Health Canada (HC)	
Industry Canada (IC)	
Office of Critical Infrastructure Protection and Emergency Preparedness (OCIEP)	
Privy Council Office (PCO)	
Public Works and Government Services Canada (PWGSC)	
Royal Canadian Mounted Police (RCMP)	
Solicitor General (SGC)	
Transport Canada (TC)	

State and Local Agencies
American Red Cross of Greater Chicago (ARCGC)
Chicago Department of the Environment (CDOE)
Chicago Department of Public Health (CDPH)
Chicago Fire Department (CFD)
Chicago Office of Emergency Management and Communications (OEMC)
City of Bellevue
Cook County Sheriff's Office (CCSO)
Cook County Sheriff's Office Emergency Management Agency (CCSO EMA)
Cook County Department of Public Health (CCDPH)
DuPage County Office of Emergency Management (DCOEM)
DuPage County Health Department (DCHD)
Illinois Department of Public Health (IDPH)
Illinois Emergency Management Agency (IEMA)
Illinois Hospital Association (IHA)
Illinois Office of the State Fire Marshal
Illinois State Fire Chiefs Association
Illinois State Police (ISP)
Illinois Commerce Commission (ICC)
Illinois Department of Transportation (IDOT)
Illinois Department of Human Services (IDHS)
Kane County Office of Emergency Management (KCOEM)
Kane County Health Department (KCHD)
King County Fire Chiefs Association (KCFCFA)
King County Government (KCG)
King County Office of Emergency Management (KCOEM)
King County Police Chiefs Association (KCPCA)
Public Health – Seattle and King County
Lake County Emergency Management Agency (LCEMA)
Lake County Health Department (LCHD)
Lake County Fire Department Specialized Response Team
Metropolitan Chicago Healthcare Council (MCHC)
Office of the Governor of the State of Illinois
Office of the Governor of the State of Washington
Office of the Mayor of the City of Chicago

State and Local Agencies (Continued)
Office of the Mayor of the City of Seattle
Port of Seattle
Seattle Fire Department (SFD)
Seattle Emergency Management (SEM)
Seattle Police Department (SPD)
Washington State Department of Agriculture (WSDA)
Washington State Department of Ecology (WSDE)
Washington State Department of Health (WSDH)
Washington State Department of Information Services (WSDIS)
Washington State Department of Transportation (WSDOT)
Washington State Emergency Management Department (WSEMD)
Washington State Ferries (WSF)
Washington State Patrol (WSP)



This page intentionally left blank

**Top Officials (TOPOFF)
Exercise Series:**

**TOPOFF 2 (T2)
After Action Report**

**Prepared for
U.S. Department of Homeland Security
Office for Domestic Preparedness
by AMTI and the CNA Corporation
Under Schedule Number GS-10F-0324M,
Order Number 2003F028**

This page intentionally left blank

TABLE OF CONTENTS

Summary Report | SR-1

Participating Agencies List | PAL-1

Administrative Handling Instructions | v

I.	Introduction	 1
	A. T2 Goals	1
	B. T2 Open Exercise Design and Concept	2
	C. Significant Aspects of T2	2
	D. Overview of the AAR	3
II.	Background	 5
	A. Public Law Authorizing the Top Officials Exercise Series	5
	B. Overview of FSL Agency Objectives for T2	6
	C. TOPOFF 2000	7
	D. Related Real-World Events	8
	E. The T2 Building-Block Events	9
	F. Exercise Scenario	10
	G. Evaluation Methodology	12
III.	Reconstruction of the FSE	 17
IV.	Artificialities	 25
	A. Inherent Exercise Design Artificialities	25
	B. Artificialities Specific to the T2 Design Process	27
	C. Artificialities That Arose During Exercise Play	29
V.	Special Topics	 31
	A. Alerts and Alerting:	
	<i>The Elevation of the HSAS Threat Condition to Red</i>	33
	B. Declarations and Proclamation of Disaster and Emergency	47
	C. Department of Homeland Security Play in T2:	
	<i>The Role of the Principle Federal Official</i>	55
	D. Data Collection and Coordination:	
	<i>Radiological Dispersal Device Plume Modeling and Deposition Assessment in Washington</i>	63
	E. Play Involving the Strategic National Stockpile	91
	F. Hospital Play in the Illinois Venue:	
	<i>Resources, Communications and Information Sharing during a Public Health Emergency</i>	105
	G. Decision-making under Conditions of Uncertainty:	
	<i>The Plague Outbreak in the Illinois Venue</i>	121
	H. Balancing the Safety of First Responders and the Rescue of Victims	137

VI. Analysis of the Six Core Areas	 147
I. Emergency Decision-Making and Public Policy	149
J. Emergency Public Information	161
K. Communications, Coordination, Connectivity	181
L. Jurisdiction	191
M. Resource Allocation	197
N. Anticipating the Enemy	203
VI. Comparison to TOPOFF 2000	 207
A. Design	207
B. Participants	208
C. Evaluation, and the Data to Make It Possible	208
D. Findings	208
VII. Exercise Design and Conduct Lessons Learned	 213
A. Exercise Design and Conduct Comments	213
VIII. Conclusions	 217
IX. Glossary	 221
ANNEX A	TOPOFF 2 Master Reconstruction
ANNEX B	Department of State: <i>TOPOFF 2 International/Canadian After Action Report Excerpt</i>
ANNEX C	National Capital Region: <i>Functional Exercise After Action Report</i>
ANNEX D	TOPOFF 2 CyberEx After Action Report

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is *Top Officials (TOPOFF) Exercise Series: TOPOFF 2 (T2) After Action Report*.
2. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate Canadian, U.S. Department of Homeland Security (DHS), U.S. Department of State (DOS), the State of Illinois, the State of Washington, and local/city security directives. This document is marked For Official Use Only (FOUO), and information contained herein has not been given a security classification pursuant to the criteria of an Executive Order, but this document is to be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one or more FOUO exemptions.
3. Reproduction of this document, in whole or in part, without prior approval of DHS is prohibited.
4. DHS, Office for Domestic Preparedness (ODP), and DOS, the Office of the Coordinator for Counterterrorism, cosponsored the T2 Exercise Series. Mr. Theodore Macklin (b)(6) and Mr. Corey Gruber (202-514-0284) are the ODP Points of Contact (POCs) and (b)(6) (b)(6) the Office of the Coordinator for Counterterrorism, is the POC for international play.
5. This report is intended for the use of Federal, State, and local (FSL) officials responsible for homeland security. It is intended to improve the FSL plans to prevent and respond to weapons of mass destruction by understanding the lessons learned from T2.

This page intentionally left blank

I. INTRODUCTION

Top Officials (TOPOFF) 2 (T2) was a congressionally-directed, national combating terrorism exercise. It was designed to improve the nation's domestic incident management capability by exercising the plans, policies, procedures, systems, and facilities of Federal, State, and local (FSL) response organizations against a series of integrated, geographically dispersed terrorism threats and acts. The T2 exercise was co-sponsored by the U.S. Department of Homeland Security (DHS), Office for Domestic Preparedness (ODP), and the U.S. Department of State (DOS), Office of the Coordinator for Counterterrorism.

A. T2 Goals

T2 was driven by four overarching national goals:

- To improve the nation's capacity to manage complex/extreme events;
- To create broader operating frameworks of expert domestic incident management and other systems;
- To validate FSL authorities, strategies, plans, policies, procedures, protocols, and synchronized capabilities; and
- To build a sustainable, systematic exercise process for advancing domestic preparedness.

As one of the first major projects within DHS, T2 brought together extensive inter-governmental and international participation. The U.S./Canadian aspect of T2 was designed to increase coordination and communication in response to a weapons of mass destruction (WMD) incident.¹ This cross-border play focused on several bi-lateral goals:

- To improve U.S. and Canadian top officials' understanding of the international implications of a multi-faceted WMD terrorist incident;
- To improve top officials' capability to respond in partnership to the crisis and consequence management aspects of a WMD terrorism incident;
- To build a sustainable U.S./Canadian joint exercise program in support of bi-lateral preparedness and response strategies for WMD terrorism incidents;
- To assess and strengthen partnerships between all organizations, including non-traditional partners, involved in responding to a WMD terrorism incident to improve overall crisis and consequence management capabilities;
- To exercise and assess Federal, State/Provincial, and local crisis and consequence management plans, directives, and processes for addressing cross-border WMD terrorism incidents; and

¹ Analysis of international aspects of T2 and U.S./Canadian play during the Full-Scale Exercise is provided in *Annex B* of this report.

- To conduct a joint exercise in accordance with the U.S./Canadian Smart Border Declaration and U.S./Canadian Chemical, Biological, Radiological, and Nuclear (CBRN) Guidelines.

B. T2 Open Exercise Design and Concept

The first TOPOFF exercise (TOPOFF 2000) was a single, no-notice, Full-Scale Exercise (FSE) co-chaired by the Department of Justice (DOJ) and the FEMA in May 2000. Unlike TOPOFF 2000, T2 was designed as an “open” exercise in which participants were introduced to the exercise scenario prior to the FSE through a cycle of exercise activity of increasing complexity that included:

- A series of seminars exploring acute response issues;
- The Large-Scale Game (LSG) that explored mid- and long-term recovery issues;
- An Advanced Distance Learning Exercise (ADLE) which used satellite networks to support first responder training nationwide;
- A Top Officials Seminar designed to explore top official response to terrorism incidents involving WMD; and
- An FSE that allowed top officials to join all players in response to a simulated terrorist attack with a radiological dispersal device (RDD) in Seattle, Washington and a simulated, deliberate release of Pneumonic Plague (*Yersinia pestis*) at several locations in the Chicago, Illinois, metropolitan area.

The purpose of the open exercise design was to enhance the learning and preparedness value of the exercise through a “building-block” approach, and to enable participants to develop and strengthen relationships in the national response community. Participants at all levels have stated that this was of enormous value to them.

C. Significant Aspects of T2

The T2 exercise was much more than a large-scale, WMD training exercise for civilian agencies; as the name *TOPOFF* denotes, a major component of the exercise was the involvement of top officials. The top officials playing in T2 included elected officials, such as governors and mayors, as well as non-elected officials who are at the apex of homeland security decision-making: cabinet members and other agency heads at the Federal level; police, fire, emergency management, and public health chiefs, among others, at the local level; and the directors of statewide agencies, including state police and the National Guard. The top officials were involved not only for their own learning but also to make possible realistic multi-government-level play. At the T2 After Action Conference (AAC), DHS Secretary Tom Ridge stated that the Homeland Security Council, which met repeatedly during the FSE, “dramatically increased its awareness of the nature and complexity of top-level issues related to terrorist attacks.”

The TOPOFF process...provides the nation an architecture upon which terrorism preparedness responsibilities can be played out, tested, and evaluated.

~DHS Secretary Tom Ridge

The following developments made the T2 FSE a significant national event:

- It was the first national exercise conducted since the establishment of DHS;
- It was the largest peacetime terrorism exercise ever sponsored by DHS or DOS;
- It involved the play of DHS and the new agencies and entities within DHS, such as the Transportation Security Agency, the Principle Federal Official (PFO), and the Crisis Action Team (CAT), as well those outside of DHS, such as the Department of Health and Human Services (HHS) Secretary's Emergency Response Team (SERT);
- It represented the first time—both real and within an exercise—that the Homeland Security Advisory System (HSAS) Threat Condition was raised to Red;
- It represented one of the largest mass casualty exercises to incorporate hospital play²; and
- It involved intense and sustained top official play.
- It introduced the concept of a live opposing force (OPFOR) in a national exercise which established ground rules for the involvement of a simulated active enemy threat in future exercises.
- It expanded the use of sophisticated news reporting simulation through the use of the Virtual News Network (VNN).

As a result, T2 provided an unmatched opportunity to examine domestic incident management policies, procedures, and systems, as well as an opportunity to review critical communication and coordination issues as they have evolved since TOPOFF 2000, the terrorist attacks of 9/11, and the anthrax attacks during the fall of 2001. Therefore, the results and findings of this exercise will allow agencies and organizations at all levels of government to identify problems and develop solutions. At the AAC, DHS Secretary Tom Ridge underscored the success of the T2 model as “a proven framework for bringing together all elements of DHS” and designated the TOPOFF Exercise Series as the lead exercise within DHS.

D. Overview of the AAR

This After Action Report (AAR) provides the results of the FSE analysis, and integrates the findings from pre-FSE seminars and the LSG.³ The *Background* section provides a history of the exercise scenario and a brief description of findings from TOPOFF 2000, other exercises, and real-world events that have influenced both the design and evaluation of T2. It also outlines the exercise evaluation methodology, focusing in particular on how the events of the FSE were reconstructed and analyzed. The *Reconstruction* section summarizes exercise events in the Washington and Illinois venues as well as interagency play in Washington, D.C.⁴ The next section details exercise *Artificialities*. The *Special Topics* section examines a set of events or issues (such as the elevation of the HSAS to Red) that have special significance to the response community and which fall outside of or have substantial overlap between the six, pre-determined areas of analysis. The *Analysis of the Six Core Areas* discusses the overarching issue areas identified from a review of TOPOFF 2000 and other exercise findings, FSL agency objectives for T2 submitted prior to the FSE, and real-world events such as 9/11. Included in this section is

² Sixty-four hospitals actively responded to the notional bioterrorism attack in the Illinois venue and 16 hospitals responded to the radiological event in the Washington venue.

³ The findings from the seminars, the large scale game, and the ADLE were published previously.

⁴ A searchable, detailed reconstruction of events from the WA, IL, and Interagency venues is provided in Annex A.

a summary of how the findings from the seminars and the LSG relate to the conclusions drawn from the analysis of the data collected during the FSE. The next section provides *A Comparison of T2 to TOPOFF 2000*. Lessons learned from the design and conduct of the exercise are described *Exercise Design and Conduct Lessons Learned*. In the final section of this report are the *Conclusions* drawn from the *Special Topics* and *Analysis of the Six Core Areas*.

During the FSE, DHS and DOS invited representatives from the Stanford University Center for International Security and Cooperation Institute for International Studies to observe activities in Washington, D.C.; and the Washington State and Illinois venues. Their report is included as an appendix to *Annex B*.

Two other exercises were conducted simultaneously to the T2 FSE: the TOPOFF 2 CyberEx and The National Capital Region Functional Exercise (NCRFE). The CyberEx was a functional exercise intended to examine, in an operational context, the integration of inter- and intra-governmental actions related to a large-scale cyber-attack synchronized with a terrorist WMD attack against a major urban area of the United States. The NCRFE was designed to coincide with the FSE to assist the National Capital Region jurisdictions in assessing their preparedness and coordination in response to a general attack on the nation and changes to the HSAS Threat Condition. The AAR for the CyberEx can be found in *Annex C*, and the NCRFE AAR in *Annex D*.

This AAR, along with its annexes, is designed to support the accomplishments of the exercise series goals and objectives and to provide an accurate and comprehensive portrait of the exercise conditions. The data contained within the main body of this report encompasses the direct observations of nearly 800 FSE data collectors, and the evaluation team's analysis of that information, as well as input from official FSL participants.

II. BACKGROUND

Understanding the concept driving Top Officials (TOPOFF) 2 (T2) requires a description of the Public Laws Authorizing the TOPOFF Exercise Series; Federal, State, and local (FSL) agency objectives for T2; TOPOFF 2000; related real-world events (such as the attacks of 9/11, the follow-on anthrax attacks, and other terrorist incidents); the T2 building block events; and the exercise scenario. It is also imperative to understand the evaluation methodology used to achieve the findings from the data collected during the Full-Scale Exercise (FSE).

A. Public Law Authorizing the Top Officials Exercise Series

Public Law 106-553 authorized T2, and Senate Report 106-404 outlined the concept:

*The Committee believes that **the nation will benefit from regular exercises.** In order to ensure that the collective national preparedness, as tested for the first time by TOPOFF, is continuously improved and departments and agencies know their roles and responsibilities, (...) **national-level exercise series shall be instituted.***

*This series of exercises, capitalizing on the lessons of TOPOFF, **should include a regularly scheduled sequence of increasingly challenging exercise building-blocks.** (...) It will feature the participation of key top officials at the Federal, State, and local levels. (...) This series of exercise components will also improve “crisis resistance” through opportunities to measure plans, policies and procedures required to (to provide an) effective response to a WMD terrorist incident. (...)*

*T2 (...) **will support the national strategy to combat terrorism,** and include events that assess the Nation’s crisis and consequence management capacity. It will include the involvement of Federal, State, and local top officials. The lead agency for T2 will be the Department of Homeland Security, and the exercise will be designed, developed and executed by Department of Homeland Security (DHS), Office for Domestic Preparedness (ODP)⁵.*

T2 supported the National Security Council’s Policy Coordinating Committee on Counterterrorism and National Preparedness Exercise Sub-group requirement for a large-scale, counterterrorism exercise commencing in 2002 and finishing in 2003.

Homeland Security Presidential Directive (HSPD)-5 articulates the federal incident management policy that guided the T2 exercise. HSPD-5, in part, states:

To prevent, prepare for, respond, to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management. In these efforts, with regard to domestic incidents, the United States Government treats

⁵ The T2 effort was initiated under the auspices of the Office of Domestic Preparedness (ODP) formerly part of the Department of Justice. ODP was later transferred to DHS when it was established.

crisis management and consequence management as a single, integrated function, rather than two separate functions. The Secretary of Homeland Security is the Principle Federal Official for domestic incident management.

B. Overview of Federal, State, and local Agency Objectives for T2

Participating FSL agencies were asked to submit objectives to T2 planners at the start of the exercise design cycle to ensure the exercise design would support participant objectives while also addressing national priorities. Agency objectives covered such areas as unified command, mutual aid, law enforcement investigation, mortuary services and fatality management, public information/education, surveillance, and epidemiology, among numerous others.⁶ Figure 1 demonstrates that the FSE design, as documented and executed through the Master Scenario Events List (MSEL), largely addressed FSL agency objectives. These objectives were linked to MSEL items (defined by participating agencies and described in the T2 Exercise Plan (EXPLAN)). Those objectives for which the associated MSEL item took place during the FSE are noted in the figure as being “addressed at least once,” during FSE play. Those for which the associated MSEL item did not take place are noted as “possibly not addressed” during FSE play.⁷

⁶ A detailed list of these objectives is provided as an appendix to the T2 Exercise Plan (EXPLAN).

⁷ The word “possibly” is used because just because the associated MSEL item did not occur does not necessarily mean the objective was not addressed. Each agency has determined whether its objectives were accomplished and has documented this in their respective AARs.

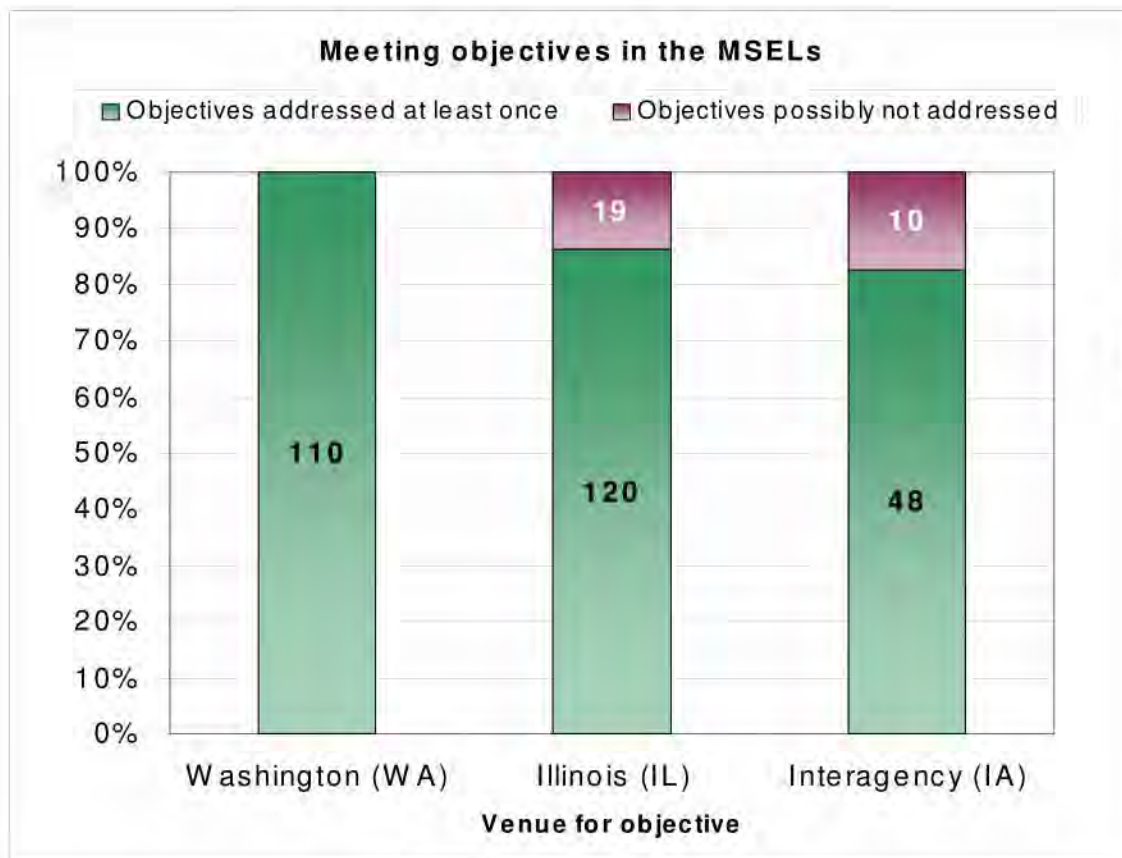


Figure 1. FSE Addressed FSL Objectives

C. TOPOFF 2000

Like T2, TOPOFF 2000 involved simulated terrorist attacks against two metropolitan regions: a chemical attack in Portsmouth, New Hampshire, and an intentional release of pneumonic plague in Denver, Colorado. Executed during May 2000, the TOPOFF 2000 FSE pre-dated the terrorist attacks of 9/11.

There were eight principle observations drawn from TOPOFF 2000:⁸

- Multiple direction and control nodes, numerous liaisons, and an increasing number of response teams complicated coordination, communications, and unity of effort;
- Threat information and a common “threat picture” were not shared or coordinated in a timely manner;
- Collaboration and methodologies in coordinating and sharing WMD hazard information and analysis need to be strengthened;
- Educating, exercising, and equipping crisis and consequence managers and responders remained a national priority need;

⁸ TOPOFF 2000 Exercise Observation Report, page EX-17.

- The response to a large-scale bioterrorism incident was significantly different from response to other WMD;
- The fragility of the public health infrastructure, reluctance to invest heavily in preparing for a low probability event, and shortfalls in current bioterrorism preparedness increased the reliance on leadership, effective response, and information management at the federal level;
- The respective and compassionate management of contaminated human remains, including legal requirements, evidentiary controls, and evidence collection, and their ultimate disposition required concerted analysis and planning; and
- The importance of joint public affairs in a WMD incident could not be overstated. The interagency public affairs community needed to continue to demonstrate an increasing capacity for joint public affairs following a WMD incident.

The success of TOPOFF 2000 was instrumental in obtaining continued funding for conduct of subsequent TOPOFF exercises. While the intent was to conduct a no-notice exercise, Congress realized the value of a building-block approach to preparedness and instructed TOPOFF planners to develop a series of exercise activities of increasing complexity. Many elements developed in TOPOFF 2000, such as the Virtual News Network (VNN), were retained and expanded for T2. TOPOFF 2000 participants initiated numerous corrective actions based upon the lessons of the exercise, and these were evident in the management of the events surrounding 9/11 and the anthrax attacks, as well as during the T2 FSE.

D. Related Real-World Events

1. 9/11

The events of 9/11 affected T2 planning, which was in the preliminary stages when the attacks occurred. In the aftermath of 9/11, the President created the Office of Homeland Security, and the Administration and Congress subsequently established DHS. Though planning for T2 was well underway by the time DHS was established, the participation of the new department became imperative, as many of the exercises' objectives centered around determining how existing procedures would be changed by a DHS-managed, federal response to incidents involving WMD.

2. Anthrax

The attacks of 9/11 were followed by mail-based anthrax attacks. These attacks served to underscore and reinforce some of the TOPOFF 2000 observations listed above in the *Background* as well as the need to exercise the nation's bioterrorism response.

3. Other real-world events

In June 2002, Attorney General John Ashcroft announced that Jose Padilla, also known as Abdullah al Muhaji, had been arrested in May, at Chicago's O'Hare International Airport, on suspicion of both association with the terrorist organization Al Qaeda and plotting with Al Qaeda to detonate a radiological dispersal device (RDD) somewhere within the United States.

In early 2003, the Department of Health and Human Services (HHS) began a nationwide program to administer smallpox vaccinations to healthcare workers.

E. The T2 Building-Block Events

It is important to understand that the T2 design involved a conscious decision to provide participants full access to the exercise scenario. This choice was made so that the scenario could be used in the T2 building-block events preceding the FSE and also to emphasize the learning process of T2.⁹

The building-block events began with the first T2 seminar, *Public Communications during a WMD Incident*, which was conducted in McLean, Virginia, from July 17 to 18, 2002. The seminar focused on both the issues that affect a government's abilities to communicate effectively with the public either directly or through the media, and also on the decisions that must be made to ensure that appropriate messages are delivered in a coordinated and timely way.

The second seminar, *National Seminar on Bioterrorism*, was held in Northbrook, Illinois, from September 17 to 18, 2002. This seminar brought together homeland security functional area leaders from FSL departments and agencies, as well as the Canadian government, to discuss issues involved in response to an unprecedented contagious bioterrorism attack.

A third seminar, *National Seminar on Radiological Dispersal Device Terrorism*, was held in Seattle, Washington, from October 16 to 17, 2002. The seminar was designed to both identify critical issues facing FSL, private sector, and international officials and also resolve key issues faced in such an attack prior to the FSE. The seminar explored how FSL and international responders prepare for the unique problems created by an RDD scenario and the best approaches to resolve these issues. The participants were from U.S. Federal departments, Canadian agencies, and State and local emergency response agencies from Illinois and Washington.

The *National Direction and Control Seminar* was conducted in conjunction with the *Advanced Distance Learning Exercise* (ADLE), which employed distance education technology to disseminate information and provide interactive training opportunities. Overall, the seminar provided an interactive forum for discussing the nation's capacity to direct and control crisis and consequence management of complex terrorist events. ADLE viewers were given the opportunity to pose questions to seminar panel members through the DHS, Office for Domestic Preparedness' Extranet Secure Portal (ESP) website.

The T2 Large-Scale Game (LSG) was developed to improve the nation's ability to manage the long-term consequences of a terrorism attack. It focused on the mid- to long-term issues that challenge FSL and international top officials and responders in the unprecedented event of a dual radiological and contagious bioterrorism attack. Participants included senior officials from U.S. FSL departments and agencies, as well as representatives from the Canadian Government.

The lessons learned from these seminars can be found in the after action reports posted on ODP's Extranet Secure Portal (ESP).

The *Top Officials Seminar* brought together Cabinet-level officials from 25 agencies and departments in a round-table discussion that served as preparation for the T2 FSE through an

⁹ While the scenario was widely known, the Master Scenario Event List (MSEL) which actually drove exercise play, was closely held and not provided to participants.

exploration of inter-governmental domestic incident management in response to WMD terrorist attacks on the United States.

The T2 FSE was played out from May 12 to May 16, 2003. The information contained within this document reconstructs and analyzes the FSE and provides recommendations for refining future operations of integrated domestic incident management.

F. Exercise Scenario

The T2 exercise scenario depicted the fictitious, foreign terrorist organization GLODO¹⁰ detonating an RDD in Seattle and releasing the Pneumonic Plague in several Chicago metropolitan area locations. There were also significant pre-exercise intelligence play, a cyber-attack, and credible threats against other locations. Key events in the exercise scenario are briefly described Table 1.

The Homeland Security Advisory System (HSAS) national threat level was notionally raised from Yellow to Orange before the FSE on D-6 in response to credible intelligence reporting suspected threat activities.

The scenario was designed to demonstrate the tiered approach to a WMD response:

- (1) Local first responder capabilities,
- (2) State emergency management capabilities,
- (3) State National Guard capabilities,
- (4) Lead Federal Agency response, and
- (5) Title 10 military support.

In the RDD scenario, the explosion took place in the Seattle, Washington, and the city was the first to respond. Seattle then called in state resources, followed by federal resources where necessary. It was not designed to require usage of Title X resources, but nonetheless demonstrated the value of the tiered response.

On D-2 in the Chicago metropolitan area, the plague agent was notionally released at three separate locations: 1) O'Hare International Airport, 2) Union Station, and 3) the United Center. Multiple people were infected at each site. Some of the plague victims watching a Chicago Blackhawks versus Vancouver Canucks hockey game at the United Center subsequently traveled to Canada.

On D-Day, the start of the FSE (STARTEX), the RDD was detonated in Seattle, killing a small number of individuals, injuring a larger number, and scattering radioactive materials around the bomb site and over a broad area as the material was transported by the wind.

On D+1, the number of admissions to Chicago metropolitan area hospitals made it clear that a major disease outbreak had begun both in the United States and in Canada (most notably in Vancouver, home of the Vancouver Canucks hockey team). By the end of D+1 a clinical diagnosis of Pneumonic Plague was made.

On D+2, with positive laboratory identification of the plague, counties in the Chicago metropolitan area mobilized their own pharmaceutical stockpile resources for distribution to the

¹⁰ The acronym for the fictional *Group for the Liberation of Orangeland and the Destruction of Others*.

local first responder community personnel. Subsequently, the Strategic National Stockpile (SNS) was mobilized, arriving in Chicago at the reception site at O'Hare International Airport.

On D+3, the SNS was deployed from O'Hare International Airport to five distribution sites within the Chicago metropolitan area.

Table 1. Overview of Scenario

EXERCISE DAY	WASHINGTON VENUE	ILLINOIS VENUE
D-6	<ul style="list-style-type: none"> Increase in hostile cyber-activity Threat condition elevated from yellow to orange 	
D-5	<ul style="list-style-type: none"> Cyber-attacks by GLODO sympathizers 	
D-4		
D-3	<ul style="list-style-type: none"> Credible threat against Columbia Generating station 	
D-2		<ul style="list-style-type: none"> Covert release of biological agent in the Chicago metropolitan area
D-1		
D-Day	<ul style="list-style-type: none"> Truck bomb explosion in Seattle Radioactive material confirmed Terrorist Radiological Dispersion Device event declared 	<ul style="list-style-type: none"> Initial patient presentation
D+1	<ul style="list-style-type: none"> Safehouse takedown¹¹ 	<ul style="list-style-type: none"> Recognition of patient increase Clinical diagnosis of plague SNS request National Disaster Medical System activated Epidemiological investigation underway
D+2	<ul style="list-style-type: none"> Marine takedown¹¹ Command Post Exercise 	<ul style="list-style-type: none"> Lab confirmation Establish Joint Information Center (JIC)/Joint Operations Center (JOC) and Regional Operations Center (ROC) SNS breakdown Illinois WMD Team Takedown¹¹ Overwhelming #s patients
D+3	<ul style="list-style-type: none"> Tabletop Exercise (Consequence Management) 	<ul style="list-style-type: none"> SNS distribution begins Midway Airport event¹¹ Takedown in Chicago¹¹ Overwhelming #s patients
D+4	<ul style="list-style-type: none"> Hotwash 	<ul style="list-style-type: none"> Hotwash

¹¹ These events were walled from the evaluation team, and therefore are not discussed in much detail in this AAR.

G. Evaluation Methodology

This section provides an overview of the T2 FSE evaluation methodology.¹² The process by which the exercise was reconstructed and analyzed is given special attention. The T2 evaluation goals were to 1) help agencies understand domestic incident management and WMD-related issues and develop solutions, and 2) support the establishment of a model for continuous learning.

These goals are consistent with the T2 national goals and those of the T2 domestic venues. As such, the evaluation methodology focused on decision and coordination processes that support the nation's top officials and the broader system of FSL agencies. Rather than evaluating participant ability and performance or specific agency-by-agency objectives, the evaluation methodology employed a detail-oriented data collection effort to reconstruct T2 exercise events followed by an analysis focusing on six pre-selected areas of analysis:

1. **Emergency Public Policy and Decision-making** encompasses the unique challenges, difficulties, and nuances faced by top officials in the initial aftermath of a terrorist WMD attack. These differ from those of natural disasters or accidents and from normal day-to-day operations.
2. **Emergency Public Information** encompasses the unique public information challenges and implications faced by top officials and their support staff in the midst of a terrorist attack involving WMD, which may differ from that of normal day-to-day operations.
3. **Communications, Coordination, and Connectivity** encompasses the challenges of exchanging information across all levels of government, information flows supporting decision-makers, and the electronic means by which information is exchanged.
4. **Jurisdiction** encompasses the issues, conflicts, or gaps in authorities and the assumptions that may arise when policies and agreements are put into practice under the uniquely challenging conditions of a terrorist attack involving WMD.
5. **Resource Allocation** encompasses the issues involving the allocation of scarce resources, as well as the management of resources committed during the response to a terrorist attack involving WMD.
6. **Anticipating the Enemy** encompasses the unique considerations that influence decision-making when there is knowledge of a potentially active enemy threat.

The After Action Report (AAR) also includes the analysis of several special topics. These topics represent events that attracted particular interest during the FSE and crossed multiple areas of analysis.

Evaluation of the FSE consisted of a three-step process:

- Step 1: **Observation and data collection** during the exercise.
- Step 2: **Reconstruction** of events and activities.
- Step 3: **Analysis** of what happened in the exercise and why, in terms of the special topics and the six core areas.

¹² A detailed presentation of the methodology can be found in the Exercise T2 Evaluation Plan (EVALPLAN).

This methodology was intentionally structured not to evaluate player performance. Instead, the purpose was to deliver knowledge to players so that they, and non-participating agencies nationwide, can improve or create FSL policies and procedures based upon the lessons of T2.

1. Observation and data collection

T2 involved an aggressive data collection strategy.¹³ Hundreds of data collectors and controllers in the field collected data. Other data were obtained by collecting the paperwork (e.g., duty logs) kept by some players in the course of executing their duties, by having a central point to which T2-related e-mails were to be sent, and by asking controllers—especially those in the control cells—to turn in their notes. In addition, the T2 evaluation team collected feedback from players at all levels of government through the use of player feedback forms. A key element in all this data-collection was time: each observation was annotated with a time at which players recorded it to have occurred. An unprecedented volume of data was collected during the course of the FSE, and was thus a tremendously successful aspect of T2.

2. Reconstruction

T2 analysts collected and organized the data submitted by players, data collectors, and controllers to use in the reconstruction and analysis of FSE play. Figure 2 illustrates the reconstruction process. Analysts reviewed data from play sources (data collected through the course of T2 play) and control sources (data collected through T2 controllers) for each venue and highlighted data points that could support analysis of what happened and why during the exercise. Play data included logs kept by players during the course of the FSE, player feedback forms, e-mails, and data collector logs. Control data, which documented the occurrence of MSEL items and ad hoc injects during play, included field controller logs, as well as data collected in the Master and Venue Control Cells during the course of the FSE.

The evaluation team received data from numerous FSL agencies and non-government organizations. These include: The Center for Disease Control and Prevention, Department of Energy, Environmental Protection Agency, Federal Bureau of Investigation, Federal Emergency Management Agency, Federal Radiological and Assessment Center, Food & Drug Administration, Department of Health and Human Services, Department of Homeland Security, Department of Housing and Urban Development, National Oceanographic and Atmospheric Administration, Nuclear Regulatory Commission, Occupational Safety and Health Administration, Department of Transportation, U.S. Coast Guard, U.S. Marshals Service, Department of Veterans Affairs, State of Illinois Emergency Operations Center (EOC), Illinois Department of Public Health, Illinois Operations Headquarters and Notifications Office, Illinois Joint Operations Center, Chicago Metropolitan Area EOCs and Public Health Departments, participating Chicago Metropolitan Area hospitals, State of Washington EOC, Washington State Department of Health, Washington Joint Information Center, Washington Joint Operation Center, Seattle and King County EOCs, Public Health Seattle/King County, Seattle Police and Fire Departments, participating Seattle and King County hospitals, and the American Red Cross.

Where applicable, analysts tagged the data collected at the FSE, and from venue Hotwashes, the After Action Conference (AAC), agency AARs, and post-FSE interviews with exercise

¹³ Also described in detail in the T2 Evaluation Plan (EVALPLAN).

participants, for instances of potentially good practices¹⁴ or challenges in the *Six Core Areas of Analysis* and the *Special Topics*. The data were then entered into two distinctive databases for each venue: one containing the electronic record of play data tagged for the six core areas, the special topics, and artificialities; one containing the electronic record of control data (see #2 in Figure 2). The play database totaled more than 20,000 lines of data for the Washington, Illinois, and Interagency venues. The control database equaled the length of the MSEL and ad hoc injects, but also documented varying controller inputs on the times events took place.

T2 Reconstruction Process

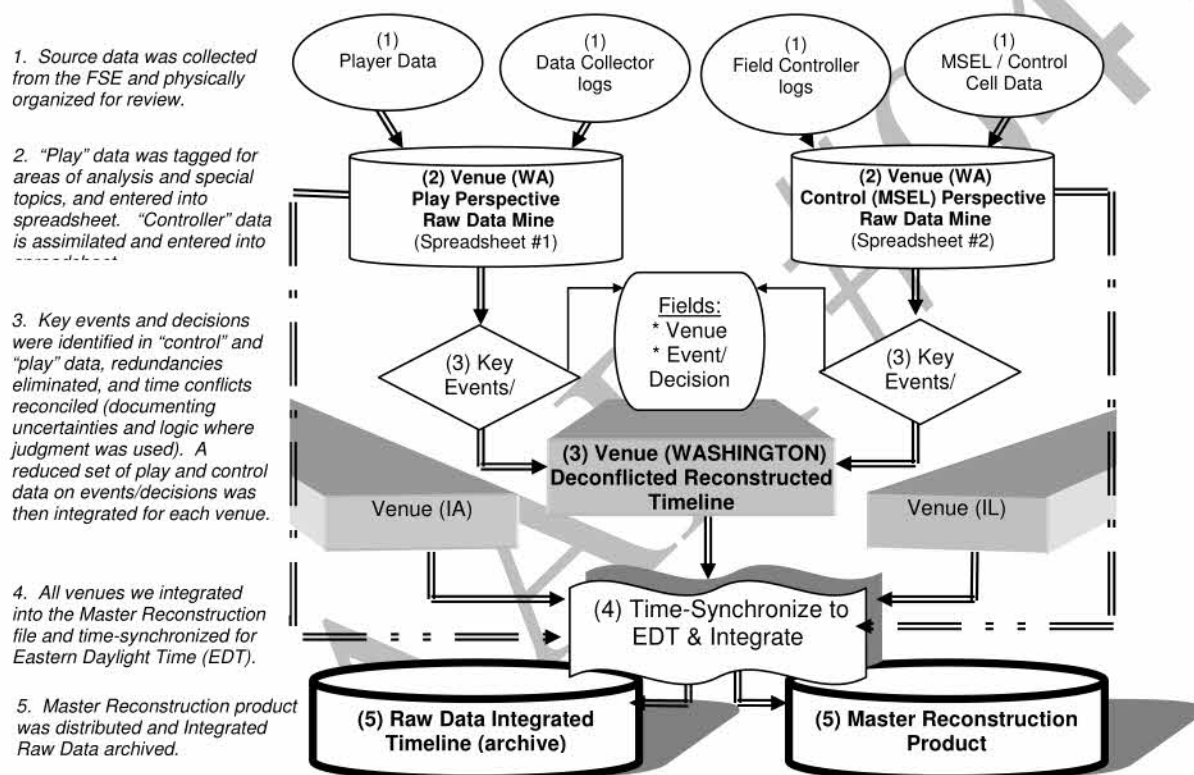


Figure 2. T2 Reconstruction Process

The analysts then reviewed the databases for each venue and identified decisions and significant events that occurred during the exercise from both the play and control data sets (see #3 in figure 2). The purpose was to filter out the innumerable events and decisions that participants faced on a daily basis, and to identify only those events that triggered top official decisions or actions.

For each data point identified as a significant event or decision, analysts researched the data to create a thorough event or decision description. For example, from one data point that read, "Susan approved the release," analysts were able to deduce from other data points recorded during relative time frames that Susan was from the Washington State Emergency Operations Center and approved a press release announcing the re-opening of local highways. Using this

¹⁴ "Good" indicates that the intent ultimately is to objectively validate it as a "best" or "exemplary" practice.

process, analysts created a comprehensive list of significant events and decisions that participants experienced during the two scenarios that were played out in the Washington and Illinois venues during the FSE. This comprehensive listing of significant events and decisions was then transferred to a new worksheet, which became the foundation for the reconstructed timeline for each specific venue.

As part of this research, analysts reviewed the various times that were noted in all the data gathered from players, controllers, and data collectors for each given event or decision and then reconciled differences. In some cases, participant records indicating when events or decisions occurred varied by hours. The analysts used their judgment to determine the most reasonable time to assign to an event when data was not available. For example, if eighty percent of people recorded an event occurring at 0900 CDT then the analysts went with the time reflected by that eighty percent and only noted the outlying times. Likewise, if accounts of when an event occurred were equally distributed with no indication of an authoritative time, the analyst determined the average of the times. Despite widely varying accounts of when an event occurred, in some cases—such as the time of the RDD explosion in Seattle—the actual time is known because it was controlled; therefore, the actual time is entered and its basis documented. The specific times for events or decisions are less important in the overall reconstruction effort than the overall sequence and flow of events. The purpose of the reconstruction is to provide an objective context for the analysis and to provide a resource to FSL agencies that describes the types of events or decisions agencies could expect to face in real-world responses to the types of terrorist WMD attacks depicted in T2.

Once the event/decision descriptions were complete and the times were reconciled for each venue, the reconstructed timelines for each venue were combined into one master reconstruction file and sorted by date and time to produce a fact-based, integrated, reconciled, objective, meaningful timeline of events for the FSE. This timeline is the basis for the analysis presented in the AAR, and is the timeline provided as *Annex A*.

3. Analysis

The analysis process is depicted in Figure 3. Analysts consulted the play and control databases, as well as inputs from participants obtained through the player feedback forms, the Hotwashes, the AAC, and Lessons Learned reports submitted by agencies during the analysis process. The AAC was designed to allow participants and planners to provide additional input to the analysis process. For each special topic (described in more detail below), analysts consulted the collected data to create a more detailed reconstruction of events and decisions occurring within that topic's frame of reference. Analysts identified and analyzed the artificialities that impacted play in these topic areas, weaving the varied, distributed, and complex pieces of each dynamic response into a single unified story. In many cases analysts followed up with participants through phone calls and emails to clarify the data collected during events, decisions, and artificialities. To lay a foundation for development of objective qualitative and quantitative measures in the future as well as lessons-learned and best practices, the analysts identified instances of good practices or challenges in the six core areas in each special topic, reviewed additional instances that were not tied to special topics, and identified findings across the exercise

T2 Analysis Process

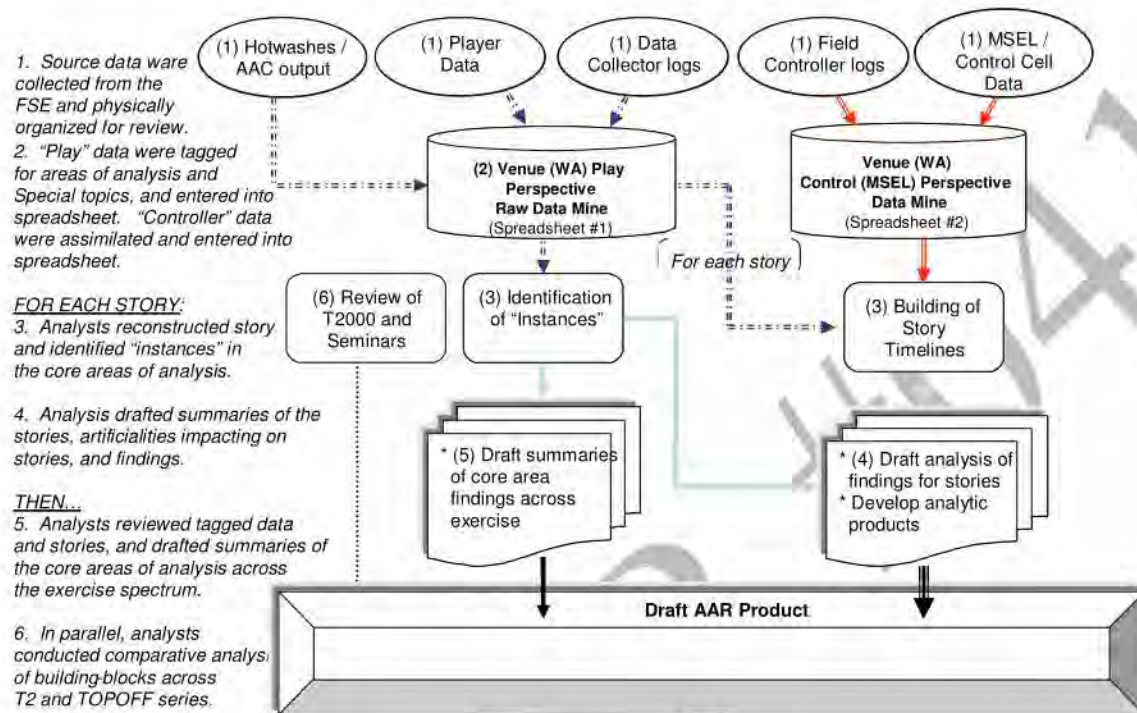


Figure 3. T2 Analysis Process

III. RECONSTRUCTION OF THE FSE

The purpose of the reconstruction was to establish an objective, fact-based timeline of the events that unfolded during the Full-Scale Exercise (FSE) as the foundation and context for analysis. The complete Top Officials (TOPOFF) 2 (T2) reconstruction product is the result of reviewing approximately 400 data collector and controller logs; thousands of player feedback forms and participant logs; many CD-ROMs; more than 2,500 emails; and hundreds of Master Scenario Events List (MSEL) items. These data sources were compiled into a spreadsheet amounting approximately 20,000 lines of data. The spreadsheet was then sorted by time, taking account each venue's specific time zone, and decisions and events were identified and filtered for redundancy.

This reconstruction, and therefore the rest of this report, does not include certain T2 activities that were partially or totally fenced off from both the analysts' view and from other events in the exercise. These include various force-on-force takedown drills; a cyber-attack exercise (CyberEx), the After Action Report (AAR) from which is published in *Annex C*; and some branch or sequel activities taking place wholly inside Canada and the National Capital Region. Furthermore, this report does not include significant data on international or Canadian play, which were collected and analyzed by the Department of State (DOS) evaluation team, the results of which are published in *Annex B*.

The activities described in this reconstruction took place in three different time zones.¹⁵ To report all in terms of their Eastern Daylight Time (EDT) equivalents would force readers with a Washington or Illinois perspective to adjust their venue's institutional memory or records with EDT; it might also distort the connotations borne by certain times (e.g., those participating in the very early hours, and those that come at the end or beginning of the workday, or at a shift change). Yet the goal is to create a unified timeline of events. Accordingly, events are presented in the order in which they happened, but narrated in terms of the local times applicable in each venue.

Events that transcended particular time zones, such as Virtual News Network (VNN) broadcasts that were seen everywhere simultaneously, are given EDT times.

It is important to distinguish between events that were physically executed in the exercise and those that were done notionally. The physical activities involved:

- Participating top officials, and those top officials who were represented by somebody else;
- Participating agencies' personnel, numbering in the thousands;
- The more than one hundred "injured" persons in Seattle, represented by role players, and augmented by a few mannequins;

¹⁵ Seattle is in the Pacific time zone; Chicago in the Central time zone, and the Washington, DC-based Interagency venue is in the Eastern time zone.

- The hundreds of role players acting the parts of the Chicago Metropolitan area patients, augmented by paper patients; and
- VNN broadcasts.

While these parties' actions were affected to some degree by exercise artificialities, they were real in the exercise sense that somebody physically participated and performed an action or actions, thereby encountering some semblance of realistic time delays, possibility of errors, and the issues that real operations entail.

All else—the closures of highways, airports, and ferry systems; orders to the population to shelter-in-place, elevations of the Homeland Security Advisory System (HSAS) Threat Condition; the spread of Pneumonic Plague outside the Chicago metropolitan area; etc.—was done in a purely notional sense. Also, all requests for emergency powers, changes of alert status, and so on were granted only on an exercise basis.

What follows is a reconstruction summary in a tabular format to lend context to the analysis. The table format affords the reader with the ability to view the events of one venue against the context of the others. Specific times are indicated based upon the data. They are provided not for the purpose of pinning events or decisions down to the exact minute, since the vast volume of data and multiple observer/participant accounts do not allow for such precision, but rather to illustrate the overall sequence of key events and decisions. Acronyms are not spelled out in the table for abbreviated readability, but all may be found in the Acronym Guide provided as a glossary to this AAR.

A complete, searchable reconstruction product is provided in *Annex A* to this AAR. It enables agencies or other interested readers to understand exactly what happened in T2, and more importantly—what types of activities and decisions one could expect to encounter in a radiological dispersal device (RDD) or bioterrorism attack from various perspectives and all government levels.

Table 2. T2 Summary Reconstruction**D-Day, Monday, May 12**

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
1200-1300 PDT	Bomb blast in Seattle. Seattle EOC activates to Level III.	Illinois EOC activates Chicago EOC activates	HHS receives message traffic from DHS, reporting the presence of Pu 229, Ce 137, and other radioactive materials in the bomb. ¹⁶ HHS reacts by officially activating the Region X REOC and sending the SERT there. SNS Operation Center activated.
1400-1500 CDT	Washington EOC activates and notifies FEMA Region X ROC.		
1500-1600 EDT	Seattle HAZMAT, responding to blast, detects radiation. FBI JOC stands-up and investigation initiated.		
1300-1400 PDT	Air, rail, highway, and ferry closures in Seattle area. Seattle and King County announce Red Alert status. Discussions of plume modeling and shelter-in-place begin. Washington requests DOE RAP assistance	Chicago increases security at likely terror targets.	DEST deployed (actually, redirected) to Seattle.
1500-1600 CDT	Rumors of National, National Capital Region, and Chicago transitions to HSAS level Red abound.		
1600-1700 EDT	Seattle implements shelter-in-place, declares State of Emergency. Governor declares State of Emergency, activates National Guard. FRMAC requested. Second bomb identified on-site. FBI HMRU arrives on-site	Lake County EOC activates. Hospitals alter command relationships. Governor increases security at nuclear power plants. DuPage County EOC begins 24-hour staffing.	DOE sends Prussian Blue to Seattle. Deputies meet 1700; Principles meet 1730.
1400-1600 PDT	Stafford Act 401 request by Governor of Washington for Declaration of Major Disaster. Shelter-in-place declared	RDD info faxed to hospitals by Chicago Department of Public Health. Public transit stepped up. Four SARS-like patients coughing up blood arrive at Edward Hospital in DuPage County.	
1600-1700 PDT	Port to Marsec 3 per USCG. DEST and PFO arrive. AMS conducts survey. FRMAC arrives		
1800-1900 CDT	DHS Secretary declares HSAS Red for Seattle, Los Angeles, San Francisco, Houston, Chicago, New York, and Washington, D.C.		
1900-2000 EDT			
2000-2400 EDT			

¹⁶ Knowledge of Pu 229 as part of the RDD this early in the exercise is an artificiality. It was not definitively identified by radiological experts in Washington State until late on May 12, 2003.

Morning of D+1, Tuesday, May 13

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
2100-2400 PDT 2300-0200 CDT 0000-0300 EDT	Formulation of plans to evacuate workers and businesses west of I-5 from shelter-in-place and re-open highways. Rubble pile declared clear. Transition RDD site from rescue site to crime scene.	First Pneumonic Plague case suspected.	
0000-0300 PDT 0200-0500 CDT 0300-0600 EDT		More apparent cases of pneumonic plague. CDC EIS team on-scene.	British Columbia CDC confirms Pneumonic Plague.
0300-0500 PDT 0500-0700 CDT 0600-0800 EDT	Debate over I-5 re-opening. Evacuation of workers and businesses west of I-5 begins. Ferries resume service except to Seattle.	SERT to increase disease surveillance.	HHS orders SERT to increase surveillance.
0500-0700 PDT 0700-0900 CDT 0800-1000 EDT	Recovery and Restoration Task Force appointed. Presidential Declaration of Major Disaster approved.	Public Health Emergency Phase I activated. Phase I automatically includes Activation of POD hospitals.	
		HHS/SCC holds conference call with Region V (Chicago) to discuss biological event.	
0700-0800 PDT 0900-1000 CDT 1000-1100 EDT	State disagrees with Mayor on re-opening I-5.	Illinois Dept. of public health conference call on clinical picture of disease. Hospitals start to see connection to United Center, O'Hare International Airport, Union Station, and Canada. VNN reports flu-like illnesses in Vancouver.	DOS stands up liaison with Canada. Border security heightened - decontamination concern. Canadians intercepting Seattle flights for possible decontamination,
	False rumors of National transition to Red Alert status abound.		
0800-0900 PDT 1000-1100 CDT 1100-1200 EDT	FDA to announce embargo on foodstuffs. Americium 241, plutonium 238, and cesium 137 confirmed in RDD. Problems with plume, road re-opening, and evacuation of those sheltering-in-place.	Chicago Public Health proposes to identify travel history of all Pneumonic Plague patients. JIC press release announces plague confirmation.	CDC Director warns against over-commitment to Seattle and Chicago. EST Level I activation
		SNS readied for release to Chicago area.	
0900-1000 PDT 1100-1200 CDT 1200-1300 EDT		United Center-Blackhawks-Vancouver connection deduced.	
	Authorities strive to get accurate counts of victims.		
	Secretary of DHS gives threat update to nation via VNN, confirms terrorist attack in Seattle.		

Afternoon of D+1, Tuesday, May 13

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
1000-1100 PDT 1200-1300 CDT 1300-1400 EDT	FBI investigation of crime continues. FRMAC beginning to develop long-term assessment and monitoring plan with EPA and HHS. Disagreements over need for, and utility of, Prussian Blue in combating radiation.	Environmental samples taken at O'Hare, Union Station, and United Center. IDPH Lab confirms plague bacterium samples from patient. Governor declares State of Emergency and requests activation of the SNS. IDPH declares Phase II Public Health Emergency to ensure authorization of certain emergency procedures Emergency. Lake County declares disaster.	State Department standing up JTF w/ CAN to work border and flight issues. Need to inform receiving countries that there may be a health problem in Chicago. HHS ASPHEP suggests plague was intentionally released, and suggests a look at the ventilator situation.
	VNN has DHS Secretary in telephone interview. He announces preliminary diagnosis of flu-like symptoms as "plague." VNN asks him what people in Code Red cities should do. Secretary articulates "snowday" concept.		
1100-1200 PDT 1300-1400 CDT 1400-1500 EDT	Teams of specialists search rubble.	Governor advised to request a National Medical Disaster System to get Federal assistance; mobilizes IEMA. Port of Chicago closed.	
1200-1400 PDT 1400-1600 CDT 1500-1700 EDT	Agricultural precautions announced. Detailed plan developed for shelter-in-place zone: those east of I-5 are released; those remaining west of I-5 to be evacuated.	Chicago and Cook County sign joint Declaration of Emergency..	CDC confirms plague. All NDMS response teams been activated for possible deployment. DHS Secretary recommends lifting transportation restrictions on airports and ferries in WA; HHS, DOE, EPA agree.
1300-1500 PDT 1600-1700 CDT 1700-1800 EDT		O'Hare International Airport closed (except to receive SNS). No school in Chicago.	HHS Secretary declares a public health emergency in the City of Chicago, allowing the department to provide Federal health assistance under its own authority.
	In press conference, DHS Secretary announces HSAS Red for entire Nation; plague in Illinois		
1500-1600 PDT 1700-1800 CDT 1800-1900 EDT	Shelter-in-place zone gradually being downsized.	Governor of Illinois sends letter to the President through FEMA Region V Regional Director requesting Major Disaster Declaration. All water, air, bus, rail, interstate traffic curtailed.	
1600-2200 PDT 1800-2400 CDT 1900-0100 EDT	King County announces implementation of snow-day like regime without specifically identifying or using the term "snow day." I-90 is open; I-5 open to through traffic.	FBI investigation initiated..	DHS/EPR/FEMA Headquarters recommends to DHS Secretary and the President that an Emergency Declaration be made in Illinois rather than a Major Disaster Declaration.

Morning and afternoon of D+2, Wednesday, May 14

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
2200-0600 PDT 0000-0800 CDT 0100-0900 EDT		Steep rise in respiratory cases showing up at hospitals. Question arises as to whether pending local declarations are necessary given the IL Governor's declaration of a State of Emergency.	FEMA conference call with Regions to discuss numerous State inquiries regarding SNS push packages. TSA/FRA/STB conflict over authority to shut down rail traffic.
DHS Secretary goes on VNN and confirms the disease outbreak as plague, with a terrorist origin.			
0600-0800 PDT 0800-1000 CDT 0900-1100 EDT		IDPH director authorizes distribution of drugs to first responders. National Disaster Medical System (NDMS) requested. Governor recommends that non-essential workers stay home and that public gatherings be cancelled. Counties declare emergency and "snow day." Plague's origin at O'Hare, Union Station, and United Center confirmed. DuPage County begins distribution of its pharmaceutical stockpile to first responders	
0800-0900 PDT 1000-1100 CDT 1100-1200 EDT	SeaTac, King County, Renton, and Paine Field airports re-opened with restrictions.	Governor suspends HIPPA, Blood Bank Act, and EMS Act, [Hospital] Licensing Act, and confidentiality of health statistics. SNS lands at O'Hare.	
0900-1000 PDT 1100-1200 CDT 1200-1300 EDT	City confronts problem of contaminated fire engines and police cars.	DMORT arrive at Hines VA Hospital. Eighteen hospitals at maximum capacity. Persons who have been at one of three epicenters advised to get prophylaxis. FBI JOC opens.	
1000-1200 PDT 1200-1400 CDT 1300-1500 EDT	USCG/FBI takedown of terrorists. Shelter-in-place zone now evacuated, re-named "exclusionary zone," inasmuch as it has been fully evacuated. AMTRAK announces contamination of passenger rail cars. USCG lifts no-sail order. Misgivings and arguments over exclusionary zone; some want to expand it, others to end it. Little radiation data. Agricultural control areas and check-points established.	Presidential Declaration of Emergency approved. Concern about level of demand relative to antibiotic supply. Chicago Office of Emergency Management requests National Guard. Area counties and Chicago begin to receive and break down SNS shipments. Area State parks closed. Many hospitals have no beds and/or are locked down against crowds.	Canada says that they have quarantined all those on flight from Chicago that brought plague to Vancouver.
Casualty estimates developed.			

Evening of D+2, Wednesday, May 14

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
1400-1700 PDT 1600-1900 CDT 1700-2000 EDT	New radiological readings indicate that DOH may recommend re-closing I-5 and I-90. National Guard activates 500 troops to support law enforcement.	25 refrigerated trucks called up to be used as morgues. Counties begin prophylaxis of first responders.	
1700-2100 PDT 1900-2300 CDT 2000-2400 EDT		Some counties close dispensing down for the night. VMI begins arriving in-State.	

D+3, Thursday, May 15

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
2100-0500 PDT 2300-0800 CDT 0000-0900 EDT	Transportation restrictions lifted except in vicinity of nuclear plant.	Public activities curtailed until at least 1800 PDT. Interstate transportation still closed. FBI takedown of terrorists and terrorist lab.	Defense coordinating officers deployed to Seattle and Chicago. Increased security on incoming containers.
0500- ENDEX PDT 0800- ENDEX CDT 0900- ENDEX EDT		All SNS distribution sites open to the public. Mixed messages as to who should seek treatment. Plague bacteria reported still present at the three suspected release sites. Mixed messages on re-opening of the release sites. Non-terrorist-related crash at Midway. FBI investigation continues to ENDEX.	DOE requests activation of the VA Medical Emergency Radiological Response Team (MERRT).
Transition back to HSAS Orange, except for Chicago and New York City.			

This page intentionally left blank

IV. ARTIFICIALITIES

Artificialities are manifestations of the exercise's non-real nature. As such, they are unavoidable, and not indications of a problem. However, false conclusions can arise if their natures and effects are not appreciated. This section focuses on the key artificialities that need to be understood to draw the appropriate conclusions from the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE). Exercise artificialities are placed in three broad categories:

- Those that are inherent to the exercise design process;
- Those specifically related to the T2 exercise design; and
- Those that arose during actual exercise play.

The net impact of artificialities can be difficult to assess. For example, considerations must be taken into account for questions such as *did a particular artificiality make the response decisions or actions easier than they might have been*, or *did they unnecessarily complicate the response relative to a real-world operation*? For their part, the T2 exercise designers tried to strike a balance, compensating for one artificiality (e.g., a response team's need, absent a real emergency, to take a commercial flight) with another (e.g., the same team's seemingly premature departure).

Two questions to ask when considering an exercise artificiality are:

- What difference did it make to the participants' play; and
- What difference did it make to top officials' play?

A. Inherent Exercise Design Artificialities

Artificialities surface in any exercise involving the response to a (WMD event. The fundamental issue is that it is often impossible to exercise the full scope of a real-world event—ranging from an actual bomb detonation to shutting down transportation infrastructure to commanding the full-time attention of top officials. The result is that many exercise events or actions must be notional, or simulated, instead of actual. Despite the notional character of some events, government agencies and organizations played as though the events actually took place. This allowed the T2 evaluation team to examine critical decision-making and communication issues. In summary, as long as they are understood and accounted for in the analysis process, these limitations need not have a significant impact on interpreting the results of the exercise.

1. Top officials' play

By any standard, top official involvement in T2 was extensive. But in a real-life emergencies of the same magnitude of those portrayed in T2 top officials would be immersed in coping with the emergency, almost to the exclusion of all other activities, whereas even in T2, top officials were present only intermittently and largely on a schedule. In fact, the ability to schedule top official play was one of the reasons for pre-scripting some aspects of the exercise. Top officials devoted considerable personal time to the exercise. Some also designated individuals (e.g., a deputy) to

play their parts in the game when they were not available. The T2 evaluation team believes that top official play during the FSE was, on the whole, relatively unaffected by these artificialities of scheduling, availability, and substitution.

2. Limited scope of play

Many effects associated with a radiological dispersal device (RDD) explosion and the intentional release of Pneumonic Plague were not designed into or played in the exercise. Some of the most important include:

- Transportation gridlock in both Chicago and Seattle;
- Increased security manpower requirements resulting from the attacks, as well as the elevation of the Homeland Security Advisory System (HSAS) to Red; and
- The potential for population disruption, movement, anxiety, and fear.

Many of these are nearly impossible to simulate or would have unacceptable impacts on non-exercise participants.

3. Notional actions

Because of limits on the scope of play, the most apparent artificialities were those in which notional (or constructive) actions replaced real ones. Examples include the notional closure of I-5 near the Seattle RDD site and the use of paper patients in the Chicago metropolitan area hospitals.

4. Limited public involvement

In a real event, the public reaction can include clamor for more information, crowds of people who have fled their homes, traffic jams, or disruptive reactions at top officials' public appearances. Although T2 had people to role play patients in the Chicago metropolitan area hospitals and persons injured by the blast in Seattle, the general public was minimally represented, so reactions on the part of the public simply did not occur.¹⁷ Neither traffic jams nor public demonstrations would be feasible, from a practical standpoint. Inasmuch as these could have an impact on the top officials' decision-making, and perhaps even on the actions of emergency personnel at the scene, to preclude their existence was to introduce a necessary artificiality.

The Washington venue did have a shelter facility set up at the White Center (a county recreation facility), through which many people passed, and three other shelters (one in Seattle and two in King County) were operated on a constructive basis (i.e., no refugee role players), but these activities were scripted and did not entail the important aspect of responding to an emerging public reaction.

Many important considerations would include but not be limited to those regarding public information, heightened public anxiety, and other psychosocial factors. Such issues would expand beyond the immediate affected communities. For example, other cities in America, not coping with an on-going emergency, would look for guidance regarding what might later happen

¹⁷ Public awareness of T2 in Seattle did result in some outcry, such as some threatening-looking signs, of which nothing ever came.

in their cities. The lack of involvement from 48 non-affected states and hundreds of non-affected cities is an artificiality that must be taken into account when considering national top officials play.

B. Artificialities Specific to the T2 Design Process

The artificialities in this section either represent deliberate choices made during the design of T2 or are specific to this particular exercise (as opposed to exercises in general). These choices were made with the understanding that they would have impacts on exercise findings. The T2 evaluation team believes that these impacts are accounted for in the exercise analysis.

1. The known scenario

T2 was designed as a building-block process whereby the general exercise scenario was explored in a series of seminars, a large-scale game, and an Advanced Distance Learning Exercise (ADLE). This process was designed to promote learning among the agencies and organizations involved in T2 and, indeed, participants felt that they had learned a great deal even without the benefit of the FSE. It is important to note, however, that while the scenario was known, participants were not afforded access to the Master Scenario Event List (MSEL), which drove the FSE play.

There was some post-exercise criticism in the media about the overly scripted nature of T2 and the lack of free play. However, this turns out to be largely unfounded criticism. Figure 4 compares the times at which events in the MSEL were supposed to occur versus when they actually occurred. The figure shows that there was a substantial amount of free play.

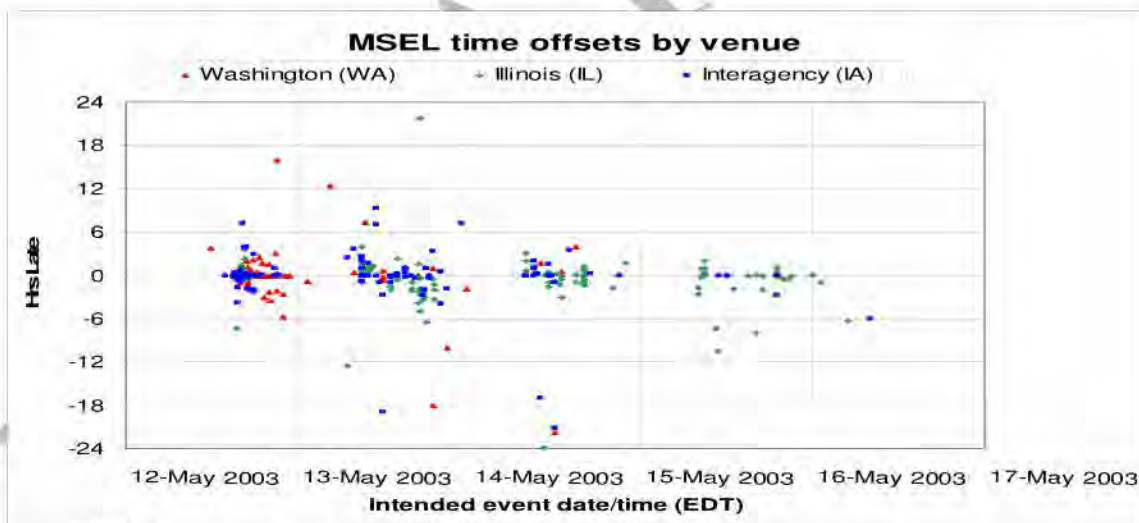


Figure 4. Variance of Events from MSEL Times

2. Scope of participation

A number of important organizations and governments were simulated. Two notable ones were the World Health Organization and the Government of Mexico.

3. VNN

Prior to the FSE, the Virtual News Network (VNN) staff and director repeatedly made the point that during the FSE VNN would be a reporter of the news, not a news-gatherer. But the full import of this policy was not clear to many until after the FSE was underway: prior to that time, some players appeared to assume that VNN would in some fashion seek out news, as well as report it.

VNN reporting was principally based upon assuming that MSEL events would happen as scheduled: reports (many of them included at the bottom-of-the-screen, known within the media as “crawlers”) were put on screen straight from the MSEL, without any news-gathering to determine whether or not they had actually taken place. This practice resulted in at least one instance in which an event was reported before it actually took place.¹⁸ Reactions to these events may have created some chains of anomalous events, but the effects do not appear to have been severe.

Some VNN coverage (e.g., some top officials’ interviews) was by necessity pre-constructed and indicative of the MSEL, and thus did not accurately portray how the scenario was unfolding. Again, this style of coverage was completely consistent with VNN’s prior self-characterization as “a news-reporting, not a news-gathering” organization.

Finally, the players—particularly those involved with Public Information—did not find themselves in a completely realistic media environment of reporters demanding the answers to questions. Only in news conferences did any such behavior occur, and even there it was not played to the degree of a real-world catastrophic event.

4. Spread of the Pneumonic Plague

Two key issues were not played in the T2 exercise: the actual epidemiological investigation required to pinpoint the location where individuals were initially infected and the impact of counter-measures (prophylaxis, population movement control measures) on the spread of the disease. In the former case, while the large number of infected individuals who attended a hockey game at United Center would have been a strong clue, the much smaller numbers infected at the transportation hubs could have been a greater challenge. In the latter case, the exercise ended before the counter-measures could have had their full impact on suppressing the transmission of the disease.¹⁹

The secondary population in a real epidemic largely consists of people who were in close contact with the primary population—family members, co-workers, and health care workers. In the T2 scenario, the secondary population was constructed on a geographical basis: the numbers of secondary cases in the Chicago metropolitan area and in the collar counties were proportional to the numbers of primary cases in each of those areas, but the association was no closer and the secondary population did not consist of close associates of the primary cases—family members, co-workers, health-care workers, and other first responders such as Emergency Medical Services workers.

¹⁸ The RDD explosion itself was one such instance: it was scheduled for 1458 EDT (1158 PDT) in the MSEL, and VNN began to report on it at that time, but it did not actually occur until ten minutes later.

¹⁹ At any rate, the exercise epidemiological profile was not developed to allow for the impact of counter-measures even if the exercise had lasted longer.

T2 did not have a tertiary population of cases, principally because the duration of the FSE was not as long as would have been needed for a set of tertiary cases to incubate and be present. Were a tertiary population to have been played, the secondary population role of healthcare workers would have been of the greatest importance, since this large secondary population would be important to spread of disease to the tertiary population. To the degree that the disease would have been spread within the population of healthcare workers, it takes a double toll, by increasing the population of the sick and decreasing the population of those able to care for them.

5. The radiological dispersal device and Seattle weather

Real radioactive materials were not released in the exercise. For the emergency workers to be able to respond realistically to readings from their instruments, these readings had to be predetermined according to what the radiation levels would be, as functions of time and space, had an actual RDD been detonated. To predetermine these levels required atmospheric dispersion models (see also the description of these in the *Special Topics* section) to run in advance, which in turn required planners to make up weather prior to the FSE. FSE play was based upon this simulated weather rather than the weather that Seattle would actually experience on May 12, 2003. In addition, planners desired that the plume disperse material to the west.

6. Lack of 24-hour play

In a real emergency, activity would have continued around the clock, especially in the first 48 hours or so. During the FSE, some activities functioned around the clock, but others did not (e.g., importantly, the Seattle-area Joint Operations Center). As a result, participants were occasionally stymied when attempting to perform some function only to find that other participants were not playing at the time. These artificialities, particularly those that impacted decision-making and response activities, have been carefully noted in the exercise analysis.

7. Pre-positioning of responders

Various assets (such as teams from Department of Energy, Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), and other agencies) were pre-positioned in the venues for reasons of safety, logistics, and cost. The evaluation team was able to account for advance deployments and ensure they were accounted for in the subsequent analysis.

8. Varying Participation Schedules

Numerous city, county, and State agencies participated in the FSE at different times during exercise play. As a result some activities that would usually occur in a coordinated fashion were disjointed. This resulted in agencies reaching differing conclusions and decisions at different times thereby created some degree of confusion.

C. Artificialities That Arose During Exercise Play

A number of artificialities arose during the execution of the exercise. In an exercise as large and complex as T2, this is not an unexpected event, and they were properly accounted for in the analysis of the exercise.

1. Chicago hospital play and the Metropolitan Health Care Council

Chicago area hospitals participated enthusiastically in T2 play. Participation counted towards their accreditations' exercise requirement. The Metropolitan Chicago Healthcare Council (MCHC) was to provide role players to be Pneumonic Plague patients in area hospitals. At the same time, MCHC was to provide other role player patients, separate and apart from those participating in the FSE, for drills to be done by the hospitals as part of maintaining their accreditation.

The addition of the extra patients by MCHC was not matched by an addition of extra control personnel. Artificialities arose when safeguards put in place by the T2 designers to avoid the blending of these two role player populations were not followed. The principal result was a distortion of the Pneumonic Plague scenario, with the unrealistic and uncontrolled number of additional cases that reduced the fidelity of play for those participants engaged in tracking the progress of the outbreak. The attempt to maintain two sets of records added confusion and may also partly by the end of the day on May 13, 2003, control staffs in the Illinois and Washington, D.C. Control Cells implemented measures to mitigate the impact.

2. Issues with control

During the FSE, there were several instances in which controllers took it upon themselves to modify the scenario, and in which other exercises or events unrelated to T2 briefly were believed to be part of T2 play. Again, these instances were documented and accounted for in the analysis.

On D+2 somebody increased the threat posed by the *Yersinia pestis* plague bacterium, telling the Illinois venue players that their newest samples from the release sites contained live bacteria. *Yersinia pestis* does not survive for long outside of a host, so the presence of live bacteria at the release sites would indicate either a re-attack at the same site or a genetically modified *Yersinia pestis* that could survive lengthy exposure outside a host. In that neither a re-attack nor a modified germ was part of the scenario, the spurious report to the players qualifies as an artificiality. It had the potential to be an important one because it could have altered (but did not) the course of play and the decision-making of top officials.

The scenario contained an incident in which investigators at the RDD site were to find a bomb-like object, which their notional investigation would then reveal not to be a bomb. These events occurred, but later another controller pronounced the device to be a bomb, leading to its explosive destruction by a remote-controlled robot. The on-the-spot creation of a second bomb represented a departure from the MSEL and—because of the implication that if there could be a second bomb, there may be a third—could have altered decision-making up the chain of command.

Finally, there were several artificialities of control that occurred purely by accident, including at least two in which word of dire emergencies (e.g., the escape of a radioactive plume from a nuclear power plant in Ohio) actually leaked into FSE play from other simultaneously-running exercises, which were to remain separate from T2.

V. SPECIAL TOPICS

During the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE), several sequences of events attracted great interest as they unfolded. Many represented truly experimental and groundbreaking elements of the response to a radiological or bioterrorism attack. These elements of response tended to cut across multiple areas of analysis, and the T2 evaluation team decided that—given their salience—the best way to address them was to do so directly, telling the story and what was concluded from it. Some aspects of these stories also appear in their respective areas of analysis.

These special topics are:

- Alerts and Alerting: The Elevation of the Homeland Security Advisory System Threat Condition to Red;
- Declarations and Proclamations of Disaster and Emergency;
- Department of Homeland Security Play in T2: The Role of the Principle Federal Official;
- Data Collection and Coordination: Radiological Dispersal Device Plume Modeling and Deposition Assessment;
- Play Involving the Strategic National Stockpile;
- Hospital Play in the Illinois Venue: Resources, Communications, and Information Sharing during a Public Health Emergency;
- Decision-making under Conditions of Uncertainty: The Plague Outbreak in the Illinois Venue; and
- Balancing the Safety of First Responders and the Rescue of Victims.

Some of these topics overlap, but each account is written so that it may stand on its own.

This page intentionally left blank

A. Alerts and Alerting: The Elevation of the Homeland Security Advisory System Threat Condition to Red

1. Introduction

One of the most visible reactions to the events of 9/11 has been the creation of the color-coded Homeland Security Advisory System (HSAS). Real-world experience has included several transitions from Yellow to Orange, and back again.²⁰ The national threat level has never been lower than Yellow or higher than Orange. Since a transition to Red has not yet occurred outside of exercise play, the Top Officials (TOPOFF) 2 (T2) exercise provided an opportunity to implement and analyze the role and impact of the HSAS Threat Condition Red. The U.S. Department of Homeland Security (DHS) has initiated the HSAS Working Group to review advisory system, as directed by Homeland Security Presidential Directive (HSPD)-3 and to examine the HSAS issues observed during the T2 Full-Scale Exercise (FSE), many of which are also discussed in this After Action Report (AAR).



In the FSE the threat condition was elevated to Red on five occasions. The initial two were local elevations (King County and the City of Seattle, Washington) immediately following the RDD explosion. The others were HSAS elevations by DHS: The City of Seattle on May 12, 2003, in response to its local elevation; seven select cities late on May 12, 2003 (New York, NY; Los Angeles, CA; San Francisco, CA; Washington, D.C.; Houston, TX; Seattle, WA; and Chicago, IL); and finally, a nationwide elevation on May 13, 2003. On May 14, 2003, DHS downgraded the threat condition from Red to Orange nationwide except for New York City and Chicago.

T2 was groundbreaking in several areas with respect to the HSAS: It represented the first opportunity for agencies to experiment with the actions associated with an elevation to Red; it allowed for examination of the implications of elevating regions to Red; it included local jurisdictions raising their own threat conditions to Red; and it highlighted that additional refinement of the system is needed. This section attempts to document how these events unfolded during the T2 FSE and what happened as a result. It is intended to promote learning and improvements with the continuing implementation of the system.

2. Background

HSPD-3 established the HSAS, which is “intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response.” The system uses colors (from green to red) to define threat levels from low to severe. Table 3 shows the HSAS

²⁰ The fact that the *National Direction and Control Seminar* and the Full-Scale Exercise each took place during Orange alerts underscored to the players and others the urgency, relevance, and realism of T2, whose scenario included a transition from Yellow to Orange and up to Red.

colors, labels, and the associated risks and the protective actions Federal departments and agencies should consider with each assigned threat level.

Table 3. Homeland Security Advisory System

Color	Label	Level of Risk	Protective Action Guidelines
GREEN	LOW	Low risk of terrorist attacks	<p>Federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures they develop and implement:</p> <ul style="list-style-type: none"> Refining and exercising as appropriate preplanned protective measures; Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency protective measures; and Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.
BLUE	GUARDED	General risk of terrorist attacks	<p>In addition to the protective measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement:</p> <ul style="list-style-type: none"> Checking communications with designated emergency response or command locations; Reviewing and updating emergency response procedures; and Providing the public with any information that would strengthen its ability to act appropriately.
YELLOW	ELEVATED	Significant risk of terrorist attacks	<p>In addition to the protective measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the protective measures that they will develop and implement:</p> <ul style="list-style-type: none"> Increasing surveillance of critical locations; Coordinating emergency plans as appropriate with nearby jurisdictions; Assessing whether the precise characteristics of the threat require the further refinement of preplanned protective measures; and Implementing, as appropriate, contingency and emergency response plans.
ORANGE	HIGH	High risk of terrorist attacks	<p>In addition to the protective measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement:</p> <ul style="list-style-type: none"> Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations; Taking additional precautions at public events and possibly considering alternative venues or even cancellation; Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and Restricting threatened facility access to essential personnel only.
RED	SEVERE	Severe risk of terrorist attacks	<p>Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement:</p> <ul style="list-style-type: none"> Increasing or redirecting personnel to address critical emergency needs; Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources; Monitoring, redirecting, or constraining transportation systems; and Closing public and government facilities.

The original directive authorized the Attorney General to assign the threat condition. HSPD-5 amended HSPD-3, such that:

Threat Conditions shall be assigned by the Secretary of Homeland Security, in consultation with the Assistant to the President for Homeland Security. Except in exigent circumstances, the Secretary of Homeland Security shall seek the views of the Attorney General, and any other Federal agency heads the Secretary deems appropriate, including other members of the Homeland Security Council, on the Threat Condition to be assigned.

The greater the perceived risk of a terrorist attack, the higher the threat condition. According to HSPD-3, *risk* includes both the probability of an attack and its potential gravity. Decisions as to what Threat Condition to assign should, therefore, take both of these factors into account. HSPD-3 states that the evaluation of the Threat Condition is qualitative and shall include, but not be limited to, the following factors:

- To what degree is the threat information credible;
- To what degree is the threat information corroborated;
- To what degree is the threat specific and/or imminent; and
- How grave are the potential consequences of the threat?

HSPD-3, as amended by HSPD-5, also authorizes the Secretary of Homeland Security, in consultation with the Assistant to the President for Homeland Security, to decide whether to publicly announce the threat condition level on a case-by-case basis. Threat conditions may be assigned for the entire nation, or they may be set for a particular geographic region or industrial sector.

HSPD-3 also directs Federal agencies and departments to implement appropriate protective measures according to the threat condition. Each department and agency is responsible for developing their own protective measures, and they also retain the authorities to respond, as necessary, with their specific jurisdictions as authorized by law.

The HSAS is only binding on the executive branch of government. It does, however, encourage governors, mayors, and other leaders to review their organizations and assign protective measures to the threat conditions, in a manner consistent with that of the Federal Government. For example, some states, such as Illinois have developed formal guidelines with specific security measures that are to be implemented under each of the HSAS color codes. In Illinois, the State Emergency Operations Center (EOC) determines the appropriate response actions and security recommendations after any elevation and transmits them to county and municipal agencies. The State of Illinois exercised this system during the FSE.

3. Reconstruction

The FSE scenario called for an elevation of the nationwide threat condition from Yellow to Orange. It occurred as scheduled by controller inject at 1000 Eastern Standard Time (EDT) on May 6, 2003, in response to scripted credible and corroborated information indicating a grave and imminent terrorist threat. By contrast, the transitions that took place during the exercise from Orange to Red occurred as player actions, not as Master Scenario Events List (MSEL)

injects, and accordingly happened when the players decided it was appropriate. Figure 5 depicts the various alert elevations to Red during the FSE, including local elevations.

Homeland Security Alert Status Timeline

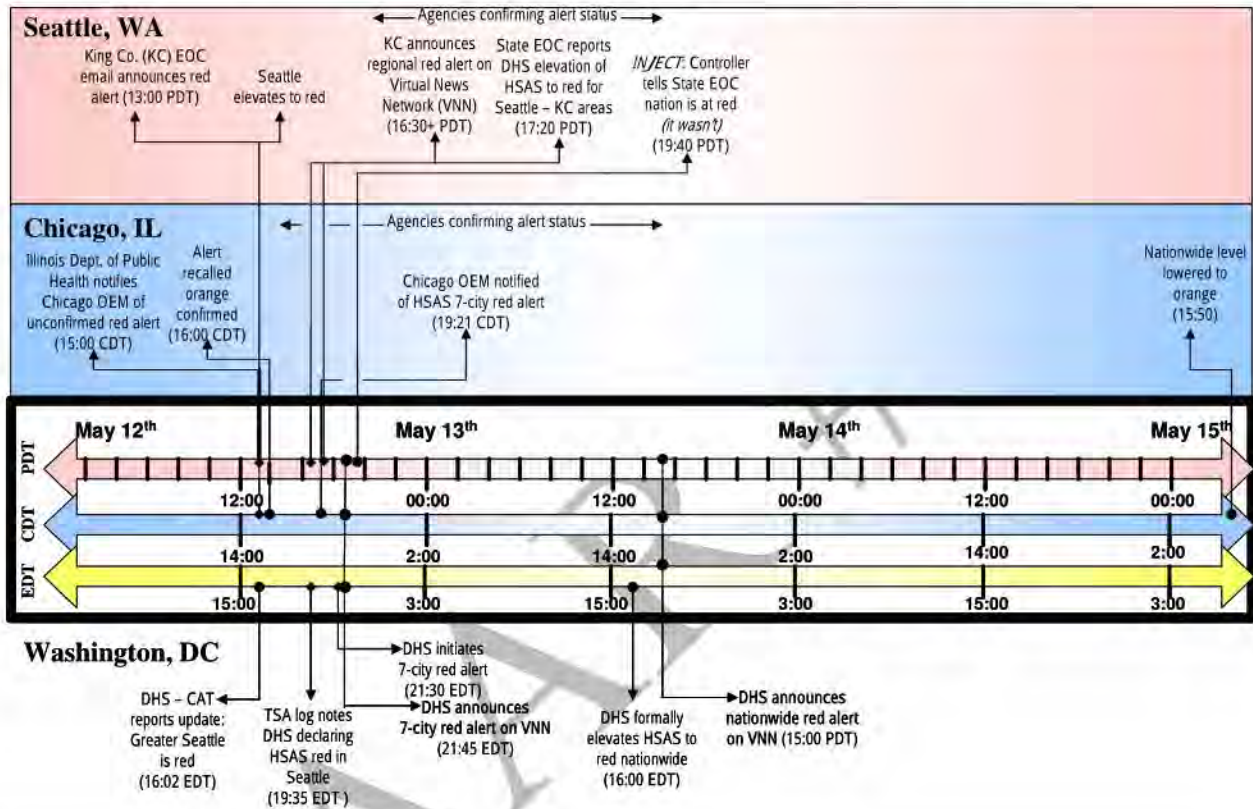


Figure 5. Homeland Security Alert Status Timeline

a. Local and regional threat condition elevations

Shortly after the radiological dispersal device (RDD) explosion, King County and the City of Seattle effectively elevated the threat condition to Red in their respective jurisdictions. The City of Seattle activated its EOC to Phase III immediately in response to the blast. The King County EOC posted its elevated threat condition at 1240 Pacific Daylight Time (PDT) on May 12, 2003 and distributed an e-mail announcing the elevation at 1319, stating, "The threat level is raised to Red." Local officials announced a regional elevation for Seattle and King County on the Virtual News Network (VNN) around 1630 PDT.

Data indicates that DHS learned of Seattle and King County's intent to raise their alert levels as early as 1600 EDT. Several data points suggest that DHS responded to this by initiating an elevation of the HSAS to Red in Seattle. The only formal documentation of this was found in a

DHS/Transportation Security Administration (TSA) log at 1935 EDT, which reported that DHS elevated the HSAS to Red in Seattle.²¹

Substantial confusion followed these first elevations. Many participants in all venues assumed the first local elevations were initiated by DHS and that they applied to the nation. Uncertainty regarding the alert status of King County, Seattle, and Washington State ensued for almost 24 hours as agencies sought to confirm the specifics. The confusion even spread to at least one of the exercise control cells. At 1940 PDT on May 12, 2003, a controller told the WA State EOC that the nation was at Red (which it was not at this time), fueling the confusion.

Meanwhile, the City of Chicago and the State of Illinois experienced brief, false elevations to Red. For example, around 1500 Central Daylight Time (CDT) on May 12, 2003, the Chicago Department of Public Health notified the Chicago Office of Emergency Management (OEM) of an unconfirmed Red Alert. The Illinois Department of Public Health (IDPH) notified the Chicago OEM of an unconfirmed Red Alert soon thereafter. This may have been triggered by the belief that the nation was elevated at the time of the Seattle/King County elevation or separate elevation within the health alert system which is also color-coded. Over the next two hours, the HSAS threat status was ultimately confirmed as Orange:

- At 1535 CDT the Director of the Chicago OEM advised that the elevation to Red was unconfirmed and gave instructions to “hold at Orange pending formal notification through the HSAS system”;
- By 1600 CDT the Chicago and State EOCs had confirmed the HSAS threat level was still at orange; and
- At 1711 CDT, the Chicago EOC distributed a message that the HSAS threat level was still Orange.

b. Seven-cities threat elevation

Later in the evening of May 12, 2003, the Secretary of DHS decided to raise the HSAS threat condition for seven cities including Seattle and Chicago based upon intelligence that indicated a severe risk of terrorist attacks in those areas. A DHS Crisis Action Team (CAT) situation report and e-mail distributed at 2030 EDT noted that:

DHS advised that effective at 2130 EDT (1930 CDT/1830 PDT) on today's date, the alert level will be raised to Code Red for the following cities: Seattle; San Francisco; Los Angeles; Houston; Chicago; New York; Washington, D.C.

Around 2145 EDT, the Secretary of DHS announced on VNN that DHS had done an assessment of the need to take additional preventative action “throughout the country” and had “raised alert in the six cities along with King County (WA), and the City of Seattle.” This appeared to be pre-coordinated by DHS with other agencies, as many entities, but not all, knew before the formal announcement on VNN. Some were still confused about the status of Illinois and Washington in light of this, and there was some confusion in the WA State EOC as to whether this applied to the City of Seattle and King County as well.

²¹ The analysis team attempted to confirm this information via phone calls but did not receive a response by the publication of this draft report.

Agencies were uncertain about the impacts of a DHS elevation of the HSAS to Red in Washington, and local jurisdictions began inquiring about “what would DHS close” and the impacts on airspace and ports, among other systems. There were some breakdowns in communication: the Principle Federal Official (PFO) in Washington noted that there were no messages coming from DHS to the Joint Information Center (JIC) or Joint Operations Center (JOC) related to this elevation prior to the VNN announcement. Also, a Federal Emergency Management Agency (FEMA) log referred to “breaches of protocol” in notification procedures.

c. Nationwide

On May 13, 2003, VNN reported between 1445 and 1545 EDT that the Secretary of DHS was considering raising the entire nation to Red. At 1530 EDT, a member of the DHS CAT noted that:

The CAT leader passed results of meeting with Secretary Ridge—he will recommend to President that all three Chicago airports...rail/trains be closed, intercity buses be closed down, mass transit will remain open, highways will remain open. Also recommended red nationwide, but transportation systems nationwide will not be closed to keep supply chains open.

The DHS Office of International Affairs received similar information from TSA.

At approximately 1600 EDT, the Secretary of DHS initiated a nationwide elevation to Threat Condition Red when it became clear that the entire country could be under attack. A DHS “ALERT AL-03-TOPOFF2-M” formal memorandum recorded this as follows:

The Secretary of DHS, in consultation with the intelligence community and the Homeland Security Council, raised national threat level to Code red nationwide as of 1600, May 13 due to the RDD detonation and the Pneumonic Plague release in Chicago and receipt of credible information that additional attacks may be planned...Federal Departments and Agencies, and State and local authorities, are directed to immediately implement protective actions identified in Operation Liberty Shield...

The Secretary of DHS appeared on VNN at 1800 hours EDT to announce the elevation of the nation to Red.

Following this news, the Illinois State EOC initiated the State of Illinois alert system and provided detailed instructions to the City of Chicago and collar counties. Using a standardized communications system and operating procedures, Illinois’ participating agencies initiated a response to the threat elevation.

The Director of the WA State EOC heard about this DHS action via VNN; he did not receive any formal notification from DHS before the Secretary’s speech. He also did not receive any written guidance about the impact on transportation systems or whether public events should be cancelled. As of 1900 PDT, top officials in the WA State EOC had still not received formal confirmation of the elevation. The Joint Operations Center (JOC) contacted King County looking for a copy of the speech or formal documentation. The Seattle and King County EOCs also learned about the elevation through VNN and expressed some frustration at the lack of formal notification.

The apparent lack of formal notification led to continued misunderstandings about the scope of DHS's action. There was some speculation in the Seattle EOC that perhaps the latest announcement applied to Chicago only: "Suspect this message was garbled and pertains to Chicago only. Request DHS fax us paper on condition of Red Statement..." At 1700, a Seattle EOC data collector noted a DHS acknowledgement that it did not follow proper notification protocols: "DHS agrees that they did not follow procedures to notify top officials..."

There was widespread confusion at all levels of government regarding the actions to take in response to the DHS elevations to Red, as well as confusion regarding the actions Federal agencies were expected to take (e.g., closing airspace). Many Federal, State, and local (FSL) agencies looked to DHS for specific guidance, as the following four examples illustrate:

1. From notes on a discussion among local top officials in the Seattle EOC of the nationwide elevation to Red on May 13, 2003:

What is working and what is not...what does stay at home for 48 hours mean? Who maintains water, power, and hospital services? etc...Will feds shut down the airports? Interstate commerce, Ports? We are not sure what 'go home for 48 hours' means? ...We need to go back to the Feds, DHS and ask for clarification on what is key and essential personnel...We need to determine what to say in a press release...

2. Late the evening of May 13, 2003, the WA State EOC formally requested guidance through DHS/FEMA on what is required under a the HSAS Threat Condition Red:

Specifically, the State needs clarification on what Protective Measures are contemplated for Federal facilities by Homeland Security ..." and "The State EOC is aware it needs to notify the public of its position based upon the Ridge position, but is not clear on what this position is.

3. From an Environmental Protection Agency EOC discussion on Condition Red at 0800 on May 13, 2003:

Security guidance says people are supposed to report to work unless otherwise notified. The question is what we tell employees. We need a decision pretty quickly as there will be panic. Action would be to call DHS for guidance on the Federal area.

4. From the Veteran's Affairs Central Office on May 13, 2003:

Does Safe Harbor address what to do when threat level increases in only certain places - clarification language to be added to op plan - we need to monitor other cities that have elected to raise threat level themselves & notify facilities...

Even within DHS there was some uncertainty of what actions to expect and guidance to issue under Condition Red:

- "The DHS Emergency Preparedness and Response (EP&R) desk requested from agency as to what is expected of the States under Threatcon red"; and
- From the Homeland Security Center Incident/Information/Operational Response Report received from FEMA Emergency Support Team (EST) on May 14, 2003, at 0255 EDT:

The FEMA EST is requesting guidance as to what are the expectations of the states under Threat Condition Red. For the record, earlier tonight, upon notification that the entire nation was at a Code Red threat level, the EST followed the checklist included in the above referenced notification to simulate play in support of TOPOFF 2. We have subsequently received an inquiry from the State of Washington as to what is expected of the states at level Red. With this e-mail, we are forwarding this to your attention as your input will be needed to best answer these questions!

d. Downgrade to Orange for most of the United States

At 1615 EDT on May 15, 2003, FEMA e-mail traffic noted that the DHS Secretary directed the nationwide HSAS Threat Condition returned to Orange except for Chicago and New York City; these two cities remained at Red.²² The first documentation of this notice within Illinois was from the Chicago Department of Health and Human Services (HHS) to the Chicago OEM at 1515 CDT. The Chicago OEM received formal notification from FEMA Region V at 1550 CDT.

4. Artificialities

- Some of the above data suggests an exercise control problem. For example, a WA State EOC shift change briefing stated, “controller inputs are not being backed by operational inputs.” This reflects a problem with the flow of information through the control and play chains. There is at least one instance of controller interference with the WA State EOC’s understanding of the threat level, which contributed to some of the confusion.²³ While players were expected to obtain information through proper channels, some of the data did suggest controller interference at various locations and times in what may have been misguided attempts to help the process.
- Not all agencies were fully staffed for the FSE as they would be under an actual threat condition of Red: A FEMA Regional Operations Center (ROC) data collector log noted:
In reality the Disaster Field Office (DFO) and ROC would be fully staffed (at the Red threat level); we would have discussions with the State, county, etc. about what they're having to deal with...
- At 1515 CDT on May 14, 2003, the Command Group at the JOC in Illinois was informed by FEMA/DHS that the threat condition had been downgraded to Orange except for Chicago and New York City. They began to implement the appropriate changes when this was retracted and they were notified that the nation was still at Red. This may have been a situation where players were outpacing the MSEL.
- The Illinois State and Chicago EOCs closed for the night at 1700 and 1800 respectively on May 12, 2003. This resulted in an artificial delay in formal transmission of the news to the collar counties of the seven-city elevation.
- The absence of an active news-gathering mechanism, described in more detail in the *Artificialities* section of this AAR, may have contributed to some confusion regarding the

²² The Washington venue was no longer playing at this time.

²³ From WA State EOC Data Collector log: “National Controller called EOC supervisor to tell him the national threat level went Red-Effective 1740. This was an inject.

elevations as well, specifically early on in local King County and the City of Seattle where local elected officials were not able to broadcast this message widely.

- The FSE did not exercise FSL agency Continuity of Operations Plans (COOP), which some agencies may have implemented had this been a real attack or if they were under a real Red Alert. Such plans involve the emergency relocation of offices to alternate facilities depending on the emergency and threat. If even a few key agencies implemented COOPs, the communications, coordination, and connectivity issues experienced by agencies during the FSE would have likely multiplied, as agencies are not familiar with other agencies' COOP procedures and these procedures are rarely exercised across the national response community.

5. Analysis

As the reconstruction makes clear, a number of critical HSAS issues arose during the FSE events. In particular, there was pervasive uncertainty over the status of threat conditions in the various jurisdictions. While some confusion was controller-induced, this does not account for the principal impact. There was uncertainty over what actions should be taken at Red. The rationale behind the elevations was not always clear to the players. Another issue apparent in the data was concern over the costs of maintaining a threat condition of Red. Finally, many critical public policy decisions were made during this period of uncertainty of threat conditions and public information on the subject was not clear.

a. Confusion about the threat condition status of jurisdictions

This is perhaps the most pervasive problem and the confusion appears to have grown with each successive elevation. When King County and Seattle first raised their local threat conditions to Red, confusion began to spread in Washington State. Many (including data collectors and, importantly, controllers²⁴) assumed that DHS had raised the HSAS for the entire nation (the HSAS Threat Condition was elevated for just Seattle). Others wondered if Washington State was at Red (it was not until the nationwide elevation was initiated by DHS). Data suggest that as late as 0245 PDT on May 13, 2003, the WA State EOC was still trying to confirm the threat condition status of Seattle at Red and Washington State at Orange. The Washington National Guard log and JIC data collector logs finally confirmed a consistent understanding of threat status for the city, county, state, and nation by 0737 PDT on May 13, 2003, (Seattle and King County were Red, and the state and nation were Orange). Many assumed again the entire nation was elevated to Red when the threat status of the seven cities was elevated.

b. Confusion as to what actions to take under a red alert

During the FSE, there was widespread confusion at all levels of government regarding specific protective actions to be taken under HSAS Threat Condition Red. This included actions that should be taken by a particular agency as well as what actions others were implementing. Federal agencies such as FEMA, Department of Transportation, HHS, and others have well-developed action plans for Threat Condition Red. FEMA has checklists that have been developed, and it simulated the usage of them during the exercise. However, Federal plans do

²⁴ This is relevant to the analysis to the extent that some of the data collector accounts were inconsistent as their interpretations of messages broadcast on VNN differed as did participants. Further, controller confusion resulted in at least one false inject.

not all carry the same level of detail, and may not be widely or consistently understood by other Federal agencies, State and local governments, the private sector and the general public. Many agencies looked to DHS for clarification as to what actions they should take, and what actions the Federal Government would be taking, under a Red Alert.

The language in HSPD-5 states that the HSAS is only binding on Federal agencies and that those agencies are responsible for developing their own specific protection measures to meet the guidelines of the HSAS. Furthermore, HSPD-5 is not binding on State or local governments, but encourages them to develop their own protective action strategies. But this flexibility also means that no single agency at any Federal, State, or local level of government has a consistent and comprehensive understanding of the protective actions that might be taken by other agencies under Red. Further, the potential impacts of protective actions taken by an agency or jurisdiction on other agencies or jurisdictions are not well understood. The confusion is magnified when the Federal HSAS and State/local elevations intersect and are not synchronized. For example, Federal and State agencies in Washington were temporarily uncertain as to their status after the local Seattle and King County elevations to Red. When the nation was elevated to Red by DHS, State and local agencies were uncertain as to the impact on them.

Participants in the T2 After Action Conference (AAC) suggested the development of an escalating scale of operational response linked to the HSAS levels. This system would be defined by a federation of FSL agencies and would offer a comprehensive operational response framework that jurisdictions at all levels could use to help define their response plans for each threat level. Such an operational framework would help to increase the consistency of measures taken across the nation, while preserving the flexibility of the system overall. It would help to ensure that all jurisdictions, regardless of their potential specific decisions on how to respond to various elevations, are at least considering common families of protective measures in those decision processes.

c. Some confusion may be due to unclear language

While threat conditions under the HSAS may be set for a particular geographic area or industrial sector, it is generally referred to as the “national threat level,” possibly contributing in some cases to assumptions that it applies to the entire nation rather than specific areas. During the FSE, the term *national* in reference to the DHS Threat Condition appeared to be interpreted two different ways:

- It applied to the entire nation (which was not the case in initial HSAS elevations); and
- It referred to the national threat level recommendation system, which could apply to specific localities/jurisdictions/regions.

The term *regional* was used and interpreted in as many as five different ways:

- DHS had raised the threat condition for some regions which were not clearly specified, and which may not have been along clear jurisdictional boundaries;
- DHS raised the threat condition for one or more local jurisdictions (e.g., King County and Seattle);
- Local jurisdictions raised threat conditions on their own;

- DHS raised the alert level for certain, specific cities (e.g., when the alert level was raised for seven cities, some referred to this as a regional elevation); and
- A regional Red Alert was instituted for Washington State, while the nation was still at Orange.

d. Formal notification procedures were not consistently employed or understood

Another potential source for confusion lies in the area of communications and coordination; formal notification procedures for changes to the HSAS Threat Condition, and State/local threat conditions were not consistently implemented or well-understood across FSL levels of government. Many participants relied on informal communications. While there is some evidence of formal communications, they were obscured in many cases by the volume of independent informal communications occurring in parallel. Even organizations that are part of the formal notification chain found it difficult to confirm and validate information they were hearing amid the volume of communications.²⁵ Most participants (with the exception of DHS) received much of this information from VNN, and relied on this information in many cases. If agencies had shared a common understanding of a formal notification approach, one might have expected to see similar approaches to validate the informal reports they were receiving regarding changes in the threat condition status.

Some attempts were made to validate information, but many organizations acted on information they received through informal channels. The DHS PFO in Washington helped greatly to dispel confusion over alert elevations and to improve communications overall once he was in position by acting as a direct conduit to DHS and helping to streamline communications.

e. Concern about the financial and other costs associated with implementing and maintaining High or Severe levels of the alert system

During T2, many agencies attempted to quantify the costs of implementing Threat Condition Red and many raised this concern at the AAC. Some agencies sought to obtain reimbursement for these costs through various means. The data show that DHS was concerned about the potential unintended consequences of threat elevations including new vulnerabilities that could be created by reallocating resources from one focus to another. Some of the issues being addressed by the DHS-initiated HSAS Working Group are the economic and social implications of an elevated threat level.

f. Uncertainty over rationale for the various elevations

Uncertainty may be related to both the lack of formal notification and the lack of understanding about what protective measures to take in response at red. Some agencies argued that specific information was needed to identify what actions to take. For example, the following comment comes from the WA State EOC: “People come in all alarmed because DHS wants to go to Red Alert nationwide. No one knows why but that requires Americans to stay home for 48 hours...”

The concern about the lack of specific intelligence accompanying many real-world threat elevations was also voiced at the AAC. Some of this is due to a lack of specificity or to

²⁵ At 2146 hours PDT on 12 May 03, a FEMA ROC Data Collector reports that “the State had received a message saying all of US on Red ...been trying to track where info came from and get right info.” This same log also noted a belief that the entire nation remained at orange when by this time seven cities had been elevated to Red.

information security in source intelligence, issues currently being addressed by DHS. But increased coordination between DHS and the states and localities on the nature of threats severe enough to merit increased elevations in the threat system to their jurisdictions, particularly to Red, are crucial to a response that minimizes unintended consequences and maximizes the use of limited resources towards an increased protective posture.

g. Many public policy decisions were made during this time of uncertainty

Numerous decisions were made during this period of uncertainty—some of which would have seriously challenged the agencies' abilities to maintain credibility and implement public policy objectives given the widespread lack of understanding of the threat condition status. This could have had dramatic impacts on messages to the public as well. For example, word of an elevation to Red that was later reported to be incorrect likely would have caused some alarm. Decisions to re-open transportation corridors, such as the airspace in Seattle, would have been confusing, in light of a national condition of Red or even a continued city-wide condition of Red. The potential public policy implications of elevations to Red at all levels of government further underscore the importance of a coordinated, synchronized, operational response to HSAS elevations.

h. Public information was unclear

Many of the issues highlighted above would have had impacts on the effectiveness, comprehensiveness, and consistency of messages delivered to the public by top officials. Participants reiterated at all of the T2 seminars the importance of consistency and comprehensiveness of messages for establishing and maintaining top official and spokesperson credibility. Top officials' public announcements, while limited, did not provide specific information to the public about what to do at Red or how agency actions and protective measures differ at Red, as Threat Condition Red relates to one at Orange. The DHS Secretary's speech that elevated the national threat condition to Red did not explain why people in Topeka, Kansas (for example) could be at the same level of risk as those in the affected areas or other higher-risk areas, such as New York City. In their public announcements, State and local officials did not clarify the local nature of the initial elevation to Red and the implications therein. Further, there was no mention in any of the public announcements of a synchronized FSL agency response to the elevations (at present this is an issue as described in part *b.* of this section).

A consistent and comprehensive operational response at all levels of government would be key to building confidence in the overall protective posture. Public perception of a comprehensive and consistent operational response would be especially important for top officials if, as was the case during the FSE and the Large-Scale Game (LSG), an attack were to occur in a jurisdiction that was under an elevated threat condition. The HSAS system cannot ensure against all future attacks, and is not one hundred percent failsafe. Its value and goal is two-fold: (1) increase the overall protective posture to reduce the risk of a terrorist attack; and (2) build public confidence in the government's ability to protect the public and provide a sense of safety and security.

Both the value and goal of the HSAS and the credibility of government top officials, depend upon a comprehensive operational response at all levels, as well as the public's belief that the government is indeed doing/has done everything in its power to effectively reduce the risk of such an attack. DHS may want to consider joint press conferences in future announcements of local or regional elevations of the HSAS that include the top officials of those jurisdictions, as

well to reinforce the public's confidence that a comprehensive response is underway. Further, to the extent that any part of the country, much less the entire nation, is ever at a sufficiently severe risk of attack to merit an elevation of the HSAS to Red, top officials must explain the nature of this risk as clearly as possible without compromising national security. Such information is critical to maintaining the credibility of the HSAS system and to obtaining the desired public response to such an elevation, which is a key component (along with FSL agency protective actions) to minimizing both the likelihood and potential human consequences of an attack.

A final issue with public information was the timing and delivery of the news regarding the unprecedented elevation of the nation to Red. This news was delivered at the end of the DHS Secretary's speech after numerous other general status updates and a recap of the previous day's "seven-city" elevation. Many would expect an announcement of this magnitude and gravity to lead to such a speech. Additionally, the public was not fully engaged by the Federal Government during the exercise about what actions it should be taking as the HSAS was increased. The American Red Cross, however, did post recommended actions the public should take under the different threat levels on its website, and established a call center for guidance.

6. Conclusions

HSPD-3, amended by HSPD-5, specifically recognizes "the roles and responsibilities of State and local authorities in domestic incident management" and their "initial responsibility" for incidents. The HSAS is described as a "flexible" system with the purpose of providing a "common vocabulary," and State and local jurisdictions have been encouraged to adopt the system. It is further described as a "national framework," intended to help unify various sector-specific alert systems already in existence.

The T2 FSE highlighted that additional refinement of this system is needed. Agencies at all levels were not certain what actions to take in response to Red, or what actions were being taken by other FSL agencies. As participants at the AAC emphasized, and as the FSE demonstrated, a more common and systematic, but flexible, framework for implementing protective measures is needed. Development of an "operational response" system, tied to the escalating alert levels of the HSAS, could help increase the overall protective posture taken at each level of government, and increase the overall situational awareness of top officials across a specific jurisdiction or

SUMMARY OF CONCLUSIONS— ALERTS AND ALERTING:

HSAS elevations should be pre-coordinated and synchronized with affected states/localities. There was widespread uncertainty as to the HSAS status until the nationwide alert on May 13.

Critical public policy decisions were made during a period of uncertainty on HSAS threat status.

Top officials lacked "situational awareness" and a "common operational picture" of relative increase in civil protective posture in response to condition red. ***Agencies recommend development of a parallel system of operational response linked to the HSAS levels.***

Increased coordination is needed between DHS and states/localities on nature of threats, to minimize unintended consequences and cost-effectively increase the overall protective posture.

Agencies do not have or share consistent understanding of formal notification approaches for HSAS status changes.

Public information messages regarding HSAS elevations should be clear, consistent, and explain comprehensive FSL response actions, as well as recommended actions for the general public to take.

region. Such a common operating picture across all levels of government requires improved communication and coordination; standard terminology and pre-designated action plans or checklists for all agencies may help in this regard.

Elevations of the HSAS should be synchronized (in purpose, place, and time) with States and localities, and their elevations in-line with the HSAS—specifically when alert conditions at these levels may differ, even if temporarily. Local communities will immediately implement Red-equivalent emergency procedures in the aftermath of any attack, as was done during the FSE, but coordinating these actions with DHS and the broader HSAS framework needs additional refinement. Further, elevations of the HSAS should be closely coordinated with the affected State and local jurisdictions beforehand. An HSAS elevation to Red will have impacts upon affected States and localities—States and local jurisdictions may feel pressure to respond even if they don't perceive the threat to merit such an elevation in their particular jurisdiction. Such consultation can help to ensure that protective actions are implemented in the most cost-beneficial manner appropriate to the nature of the threat.

Agencies did not share a consistent understanding of the HSAS status of the nation or their jurisdictions until the nationwide elevation on May 13, 2003. This was due to communications issues—both the absence of a shared understanding of formal notification procedures, as well as inconsistent language. In some cases, formal notifications occurred between DHS and the states, between states and local jurisdictions, and between State/local jurisdictions and DHS. However, this was not always the case and it did not appear to occur with consistency.

While the media is sometimes the first means by which government agencies will learn of major events and threat elevations, formal notifications are imperative for transmitting information as critical as alert elevations, and certainly one to Red. Agencies must all be fluent in formal processes and know to treat anything not received through them as unconfirmed. Periods of uncertainty could delay the implementation of some protective actions and impact public information. Not only might inconsistent messages and decisions impact the credibility of elected officials, it could undermine the effectiveness of public safety campaigns. Further, the extended time spent confirming the threat status through multiple channels diverted energy from other agency priorities.

Also, language must be clear and consistent. The term *national threat level* was assumed by some to refer to any threat elevations regardless of their geographic scope or the source of the FSL action. When people heard the national level was raised, many assumed this referred to its geographic scope and assumed the entire nation was at Red when it was not. In some cases elevations initiated by local or State jurisdictions were referred to as regional elevations and people were not clear about the boundaries. Some described the seven-city elevation as a regional elevation. The precise scope and nature of threat elevations, since they may vary, need to be explicitly clear to reduce confusion.

Finally, some implications of Red, such as agencies implementing COOPs, were not played and would have further complicated operations. In the event of an attack, many agencies would implement COOPs under the HSAS Threat Condition Red. This reinforces the need to have a tightly orchestrated set of procedures that all agencies understand. Future exercises should include continuity of operations and continuity of government objectives to address these challenges as well to ensure maximum realism.

B. Declarations and Proclamation of Disaster and Emergency

1. Introduction

During the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE), several declarations and proclamations of emergencies and disasters took place. Local jurisdictions in both exercise venues invoked their authorities to declare emergencies, and requested federal assistance under the Stafford Act (see below). These requests ultimately led to a Presidential Declaration of Major Disaster in Washington and one of Emergency in Illinois. In addition, the Department of Health and Human Services (HHS) declared a Public Health Emergency in Illinois under the authorities of the Public Health Service Act. This section discusses the events that led to these declarations, as well as related issues that arose during the FSE.



2. Background

a. The Stafford Act

Stafford Act declarations generally start with a request from a governor. Requests for declarations of both emergency and major disaster must “be based on a finding that the disaster is of such severity and magnitude that effective response is beyond the capabilities of the state and the affected local governments and that Federal assistance is necessary.”²⁶ A *Major Disaster* is defined in the Stafford Act as

...any natural catastrophe (including any hurricane, tornado, storm, high water, wind driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this chapter to supplement the efforts and available resources of states, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.

States may be reimbursed for up to one hundred percent of qualifying expenses under a Presidential Declaration of Major Disaster.

An *Emergency* is defined as

...any occasion or instance for which, in the determination of the President, federal assistance is needed to supplement state and local efforts and capabilities

²⁶ The Robert T. Stafford Disaster Relief and Emergency Assistance Act, As Amended, 42 U.S.C. 5121, et seq., <http://www.fema.gov/library/stafact.shtm>.

to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.

Federal assistance under a Presidential Declaration of Emergency is limited to five million dollars except in circumstances where the President determines that:

- Continued emergency assistance is immediately required;
- There is a continuing and immediate risk to lives, property, public health, or safety; and
- Necessary assistance will not otherwise be provided on a timely basis.²⁷

Other differences include limitations in public assistance (emergencies allow only for emergency debris removal and emergency protective measures, and not for permanent repair and replacement work), disaster unemployment assistance, and crisis counseling. Here again, exceptions may be made if the President determines that additional assistance is necessary to “to save lives, protect property and public health and safety, and lessen or avert the threat of a catastrophe.”

b. Public Health Service Act

The Secretary of HHS is authorized under the Public Health Service Act, 42 United States Code (U.S.C.) 201, et seq., to declare a state of public health emergency. This declaration enables HHS to delegate its granted authority, release funds and resources to prevent the proliferation of a communicable disease, and to plan an emergency medical response in the event of a disease outbreak. HHS is authorized to manage investigative and protective efforts, enter into contracts, assemble grants, disseminate information, and coordinate all other related actions reasonably necessary to respond to the emergency. The Act gives HHS and its delegated authorities, such as the Centers for Disease Control and Prevention and the Food and Drug Administration, wide discretion and independence in the management of such efforts.

A federal declaration by HHS allows for the release of federal resources, including both money and manpower. During the FSE, as a result of the Declaration of a Public Health Emergency in Illinois and in the absence of a Presidential Declaration of an Emergency or Major Disaster there at that time, HHS enabled the activation of several DHS response assets, including the Disaster Medical Assistance Teams (DMATs) and Disaster Mortuary Operational Response Teams (DMORTs).

c. State and local proclamations

State and local authorities under conditions of disaster and emergency vary by state and locality. Authorities for the jurisdictions that participated in the FSE are summarized here for context in understanding how various declarations unfolded.

State of Washington

In Washington, the Governor may declare a state of emergency pursuant to the Revised Code of Washington (RCW) 43.06.220. Through a “Proclamation by the Governor” the Governor is authorized to create curfews and curtail public gatherings; control the manufacture, transfer or

²⁷ Section 503 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, As Amended, 42 U.S.C. 5121.

possession of flammables and explosives; prohibit the possession of firearms except within a personal residence or business; designate the dispensing of alcohol as illegal and subject other goods to similar control measures; determine the use and closures of roads and highways; and anything else the governor reasonably believes to be for the safety and welfare of the residents of the State. During the FSE, the Washington Governor authorized the Washington Emergency Management Division to establish food control areas around suspected areas, and for others to issue embargoes and perform specific kinds of inspections. In addition, the proclamation activated the National Guard.

The Emergency Management Assistance Compact Act as codified in Washington State RCW 38.10.010 et seq., provides mutual assistance between states entered into the compact in managing any emergency or disaster declared by the governor of the affected state. The philosophy behind this compact is that few disasters remain within the neat confines of jurisdictional borders, and that many states have unique resources they can contribute to a neighboring, compromised state in the event of an emergency. This Act establishes the rules for such mutual cooperation in emergency-related activities.

A county may, and in the event of a Presidential Declaration must, issue a local proclamation of emergency. During the FSE, King County released a proclamation on May 12, 2003 at 1351 PDT pursuant to RCW 38.52 and King County Charter (K.C.C.) Chapter 12.52, stating that due to an explosion, the presence of radiation and other related hazards, additional steps had to be taken to protect the life and property of the county's citizens. This authorized the designated departments of King County to enter into contracts and incur obligations necessary to combat the emergency at hand.

Finally, the Mayor of Seattle may declare a civil emergency through a local proclamation of civil emergency order and did so during the FSE on May 12, 2003, immediately after the explosion, in accordance with the Seattle Municipal Code, Chapter 10.02, the Charter of the City of Seattle, Article V, Section 2, and RCW Chapter 38.52. It, too, serves the purpose of releasing funds and delegating authority in an emergency situation. During the FSE, the proclamation delegated authority to city department heads (e.g., the police chief) so that the Mayor could coordinate the overall response effort. Additionally, the proclamation notified the public of conditions where the exercise of certain rights may be curtailed, but only to the extent that the conditions make it necessary. A copy of the order was both made public and delivered to the governor of Washington and to the King County executive.

State of Illinois

Pursuant to the Illinois Emergency Management Agency Act²⁸, Chapter 20 of the Illinois Compiled Statutes, section 3305/7 (20 ILCS 3305/ 7), the Governor may declare by proclamation that a disaster exists. *Disaster* means, in relevant part:

...an occurrence or threat of widespread or severe damage, injury or loss of life or property resulting from any natural or technological cause, including but not limited to explosion, riot, hostile military or paramilitary action, or acts of domestic terrorism" (20 ILCS 3305/4).

²⁸ Illinois ratified the Emergency Management Assistance Compact Act and codified it as 45 ILCS 151/5 (2203).

The Governor proclaimed a state of emergency for the greater Chicago area on May 13, 2003, at 1230 CDT. Upon such a proclamation, the Governor may exercise designated emergency powers for 30 days. Among these emergency powers are the abilities to suspend provisions of any regulatory statutes or procedures for state business; to utilize all available state resources; to transfer the direction, personnel, or function of state departments facilitating disaster response; to take possession of personal property; to recommend evacuation, and so on. The proclamation of disaster also activates the state emergency operations plan.

An Illinois county may declare a local disaster as determined by 20 ILCS 3305/11. A declaration may only be made by a principal executive officer of a political subdivision (i.e., a county) or by his/her interim emergency successor and cannot be continued in excess of seven days except with the consent of the governing board of the political subdivision. The effect of the declaration of a local disaster is to activate the emergency operations plan of that political subdivision and to authorize the furnishing of aid and assistance. The Illinois data indicated that four Illinois counties declared a local disaster at one point or another and decided to consolidate the announcement of the declarations into one.

3. Reconstruction

Figure 6 depicts the timeline of the various proclamations and declarations of emergency and disaster that occurred during the FSE.

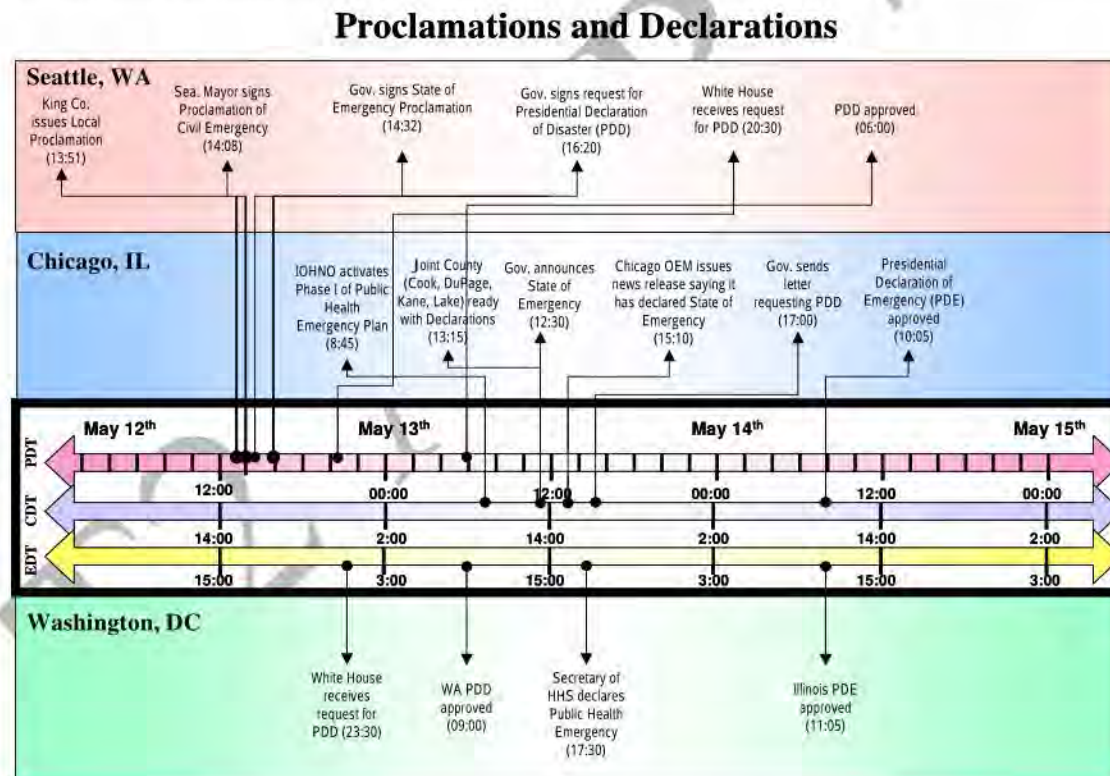


Figure 6. Proclamations and Declarations

a. Washington venue (all times Pacific Daylight Time)

In Washington State, local authorities initiated proclamations of civil emergency immediately after the explosion which occurred just after noon PDT on May 12, 2003. A primary purpose of the local proclamations was to bring in resources from outside the city and county, above and beyond those accessible through existing mutual aid agreements with emergency services departments in neighboring jurisdictions.

Shortly thereafter, the governor signed a proclamation declaring a state of emergency in western Washington, authorizing the establishment of food control areas and food embargoes by the Washington State Department of Health and Agriculture. The State Emergency Operations Center (EOC) received a copy of the proclamation at 1432 PDT, and it was forwarded to the Joint Operations Center by 1446 PDT.

The WA Governor signed a request for a declaration of major disaster under authorities of the Stafford Act at 1620 PDT on May 12, 2003. This request was received by the White House at 2330 EDT, and signed by the President (notional) at 0900 EDT on May 13, 2003.

b. Illinois venue (all times Central Daylight Time)

In contrast to the explosion in Washington, the disaster unfolded silently in Illinois. Cases of a mysterious respiratory illness first appeared on May 12, 2003. The first awareness of a potential pattern was observed around 1730 CDT on May 12 when the Pro-Net surveillance system²⁹ noted a cluster of respiratory cases at Edward Hospital in DuPage County. The illness was presumptively diagnosed as Pneumonic Plague on the morning of May 13 as cases began to mount, and a bioterrorism attack was suspected. Illinois Operational Headquarters and Notification Office soon thereafter activated Phase I of the Public Health Emergency Plan.

Just after noon CDT on May 13, 2003, the Chicago Director of the Office of Emergency Management (OEM) recommended a declaration for a state of emergency in Chicago, which authorized the city to take necessary actions, such as ordering people to shelter-in-place. Meanwhile, Cook, DuPage, Kane, and Lake Counties (the “collar” counties surrounding the City of Chicago) were initiating county-level declarations of emergency as well, and, together with FEMA, discussed whether to issue a joint declaration of disaster. The collar counties agreed that news of the county declarations should be announced jointly. At about the same time the IL Governor signed the Proclamation of a State of Emergency for Illinois. There was some question as to whether this proclamation made local proclamations of emergency moot, though they ultimately realized that local declarations were required to initiate local emergency authorities. A joint Chicago/Cook County Declaration of Emergency was signed at 1500 CDT and the Chicago OEM issued a news release announcing a state of emergency due to Pneumonic Plague at 1510 CDT.

At 1730 EDT on May 13, 2003, after consultations with Illinois officials and confirmation that the disease was Pneumonic Plague, the HHS Secretary declared a Public Health Emergency for Illinois. Meanwhile, the IL Governor sent a request for a Declaration of Major Disaster under the authorities of the Stafford Act to the President through FEMA Region V at 1700 CDT. Upon

²⁹ The Pro-Net surveillance system collects syndromic information from hospitals in DuPage County using a Web-based interface. The data are evaluated by software to determine if there are any unusual clusters or trends occurring. If an unusual spike in cases is detected the system alerts the local public health responders via a pager system.

receipt of the IL Governor's request for a Presidential Declaration of Major Disaster, FEMA Region V advised: "Although the Governor requested a major disaster declaration, under the Stafford Act definitions, an emergency declaration is FEMA's most appropriate immediate action." Accordingly, FEMA recommended that the President (notional) issue an emergency declaration, with "Individual Households Program and Categories A and B under Public Assistance [being] made available in the following jurisdictions: Cook (including City of Chicago), DuPage, Kane, and Lake Counties." A Presidential Declaration of Emergency was approved at 1105 EDT on May 14, 2003. There was some confusion among participants as to whether the request for a Declaration of Major Disaster was approved, but it was not.

4. Artificialities

The FSE artificialities did not substantively impact participant play or the conclusions in this topic area.

5. Analysis

The declaration of the public health emergency in the Chicago area was enacted with little confusion or difficulty in execution. However, it appeared that the state and local declaration processes in Illinois were at times confused. Members of the Illinois Emergency Management Agency and Illinois Department of Public Health for example, discussed whether a county-level declaration needed to be enacted in light of a state declaration of emergency, and there was some confusion among the collar counties as to the status of the different jurisdictions' declarations at various points in time. Also, there was some confusion in the Illinois State EOC as to whether the request for a Presidential Declaration of Major Disaster under the Stafford Act had been approved, which it had not—a Declaration of Emergency was approved.

Furthermore, although the process of obtaining a Presidential Disaster Declaration went smoothly in Washington, it was not as smooth in Illinois. Officials in Illinois requested a major disaster declaration to obtain maximum Federal assistance for the growing bioterrorism disaster, out of concern for the perceived five million dollar limit and other limits to Federal assistance in declarations of emergency. Some were unaware that the President can approve an expenditure of funds and approve services in excess of these limits under the conditions described above. For example, Illinois participants were not sure if the declaration authorized the Substance Abuse and Mental Health Services Administration (SAMHSA)/FEMA crisis counseling program. The FSE did not play out long enough to trigger the need for assistance in excess of those services allowed, or to allow for the Federal government to determine whether funds could be spent on programs not specifically named under Emergency Declarations of the Stafford Act.

It is interesting to note that the outbreak of plague in Illinois did not qualify as a major disaster by definition in the Stafford Act; biological disasters are not referenced in the Act. It is not clear from the FSE whether the difference in declaring an emergency or a major disaster would result in substantive real-world issues given the exception clauses under declarations of emergency described above.

6. Conclusions

Both of the simulated terrorist attacks in the FSE led to local declarations of emergency by multiple affected jurisdictions. The bioterrorism attack in Illinois was especially challenging in this arena with a widespread impact involving multiple counties, the City of Chicago and the State of Illinois.

Since there is no real-world precedent in which the Stafford Act has been applied to a biological disaster—or one involving non-explosive radiological, chemical, or biological weapons—it is noteworthy that during the FSE, the large-scale bioterrorism attack did not qualify as a major disaster. Future efforts, including exercises, should continue to refine the applicability of the Stafford Act to bioterrorism and other non-explosive disasters not explicitly defined by the Act, to increase Federal, State, and local (FSL) agency familiarity with its application to, and implications for, such disasters.

Finally, while the FSE did not necessarily indicate confusion with activation of the Public Health Act, or the declaration by HHS of a Public Health Emergency; the relationship between these authorities (and the resources that are brought to bear under them) and those available through the Stafford Act should continue to be exercised for maximum clarity at all levels of government.

SUMMARY OF CONCLUSIONS— DECLARATIONS:

In Washington, the proclamation and declaration processes went smoothly during the FSE. In Illinois, however, there was more confusion.

Future efforts should continue to explore the applicability of the Stafford Act to biological and other non-explosive terrorist emergencies that do not qualify as a major disaster, as currently defined by the Act.

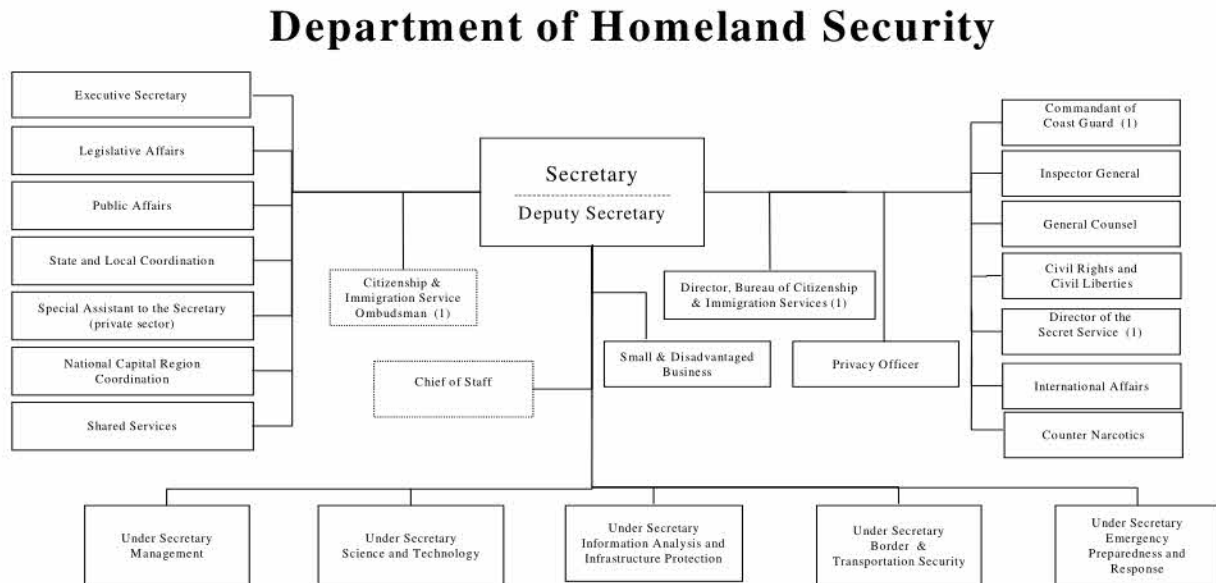
While there was little confusion regarding the activation of the Public Health Act, the relationship between it and the Stafford Act, especially the authorities and resources that are brought to bear under them, should continue to be exercised.

This page intentionally left blank

C. Department of Homeland Security Play in T2: The Role of the Principle Federal Official

1. Introduction

The Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE) was the first opportunity for the newly created Department of Homeland Security (DHS) to exercise and experiment with its organization, functions, and assets. Figure 7 depicts the organization of DHS.



Note (1): Effective March 1st, 2003

Figure 7. Organization of the U.S. Department of Homeland Security

Table 4 lists those DHS directorates, offices, and agencies for which the analysis team has data documenting their activities in the FSE. Table 4 includes, when available, a summary of the FSE activities of these organizations and the assets they deployed during the exercise. It is important to note that other DHS organizations, such as the Office of Emergency Response, played important roles in the FSE, but data collectors were not present at their Emergency Operations Centers or Headquarters.

A number of DHS emergency response assets were set up or deployed for the first time during the FSE. These include new entities that report directly to the DHS Secretary: the Crisis Action Team (CAT) and the Principle Federal Official (PFO).

During the FSE, the CAT reported to the DHS Secretary or Chief of Staff. The CAT was the Secretary's assessment and advisory team, providing the information and recommendations needed to make decisions and advise the President. In addition to the DHS directorates, offices,

and agencies listed in Table 4 that had representatives in the CAT, liaisons from the White House, Federal Bureau of Investigation (FBI), Environmental Protection Agency, and Nuclear Regulatory Commission were also stationed in the CAT. The Department of Health and Human Services (HHS) and Department of Energy (DOE) liaisons were in the DHS Homeland Security Center across the hall rather than in the CAT.³⁰ This is surprising given that DOE was the lead technical agency for the radiological response in Washington and HHS was the lead technical agency for the public health response in Illinois.³¹

The DHS Secretary designated PFOs and deployed them to the Washington and Illinois venues. The PFO's role in emergency response was first implemented during T2, and is now being codified by DHS. Based upon PFO activities during the FSE, the PFO will serve a pivotal role in the response capabilities of DHS. To further support the efforts of DHS to define the roles and responsibilities of the PFO, this section focuses on the PFO activities, interactions, and lessons learned from the FSE. Because it is focused on the activities of individuals as opposed to organizations, the reconstruction presented in this section is much briefer than that presented in other sections. It is important to note that the analysis team had an analyst with the Seattle PFO allowing for a fairly detailed reconstruction of the PFO's interactions and activities. The reconstruction and observations for the Illinois PFO are based upon information from data collectors, and as a result, a detailed timeline for the PFO activities in the Illinois venue was not developed.

³⁰ HHS had personnel limitations during this exercise due to real-world commitments, including Severe Acute Respiratory Syndrome (SARS). This resulted in a choice to staff the Homeland Security Center full-time, but meant they did not have representation in the Crisis Action Team (CAT).

³¹ For additional information about the CAT, see the *Stanford Report* in Annex B.

Table 4. Directorates, Offices, and Agencies within the Department of Homeland Security That Played in T2³²

DIRECTORATE/OFFICE/AGENCY	ACTIVITIES/ASSETS DEPLOYED
Border and Transportation Security (BTS) Directorate	<ul style="list-style-type: none"> • Bureau of Customs and Border Protection (CBP) activated the CBP Command Center • The Transportation Security Administration activated its Crisis Action Center • Immigration and Customs Enforcement/Federal Protective Services activated its Communications Center, Situation Room • Participated on Crisis Action Team (CAT)
Emergency Preparedness and Response (EPR) Directorate	<ul style="list-style-type: none"> • Activated the National Interagency Emergency Operations Center, Emergency Support Team at EPR headquarters • Deployed assets including Domestic Emergency Support Team, Federal Coordinating Officers, Mobile Emergency Response System, National Disaster Medical System, Strategic National Stockpile, and Urban Search and Rescue Incident Support Teams • Participated on CAT
Science & Technology Directorate	<ul style="list-style-type: none"> • Participated on CAT
Information Analysis and Infrastructure Protection Directorate	<ul style="list-style-type: none"> • Participated on CAT
U.S. Coast Guard	<ul style="list-style-type: none"> • Activated Crisis Action Center • Participated on CAT
U.S. Secret Service	<ul style="list-style-type: none"> • Activated Director's Crisis Action Center
Office of International Affairs	<ul style="list-style-type: none"> • Participated on CAT
Office of Legislative Affairs	<ul style="list-style-type: none"> • Participated on CAT
Office of Public Affairs	<ul style="list-style-type: none"> • Participated on CAT
Office of State and Local Government Coordination	<ul style="list-style-type: none"> • Participated on CAT
Office of National Capital Region Coordination	<ul style="list-style-type: none"> • Participated on CAT
General Counsel	<ul style="list-style-type: none"> • Participated on CAT
Private Sector	<ul style="list-style-type: none"> • Participated on CAT

³² The offices and agencies in this table represent only those for which the analysis team has data.

2. Background

The concept of a PFO is laid out in Homeland Security Presidential Directive (HSPD)-5: “the DHS Secretary is named as the PFO for the management of terrorist attacks, major disasters, and other emergencies in the United States”³³.

The duties and responsibilities of the PFO are further elaborated upon in the draft National Response Plan (NRP):³⁴

***Principle Federal Official.** The Federal official responsible for directing Federal operations in the United States to prepare for, respond to, and recover from domestic incidents; for directing the application of Federal resources in specific circumstances; and for managing any domestic incident when directed by the President.*³⁵

The draft NRP continues, stating that the DHS Secretary can name a senior Federal official as the Secretary’s senior representative at the incident. This person oversees the federal response in the field. The responsibilities of the Secretary’s representative include:

- Coordinating and synchronizing the activities of primary Federal agencies and supporting agencies;
- Overseeing the allocation of resources for response and recovery;
- Coordinating the release and distribution of information; and
- Communicating with the Secretary.³⁶

The draft NRP gives the Secretary’s representative some authorities that traditionally were those of the Federal Coordinating Officer (FCO) and the FBI Special-Agent in Charge (SAC) under the existing FRP and U.S. Government concept of operations plan (CONPLAN)³⁷.

3. Reconstruction

a. Washington venue (all times are Pacific Daylight Time)

Mike Byrne, the DHS Director of National Capital Region Coordination for Emergency Response, was appointed the PFO in Washington. Figure 8 lays out a reconstructed timeline of his activities in the Washington venue. He notionally deployed with the Domestic Emergency Support Team (DEST), prior to the radiological dispersal device (RDD) explosion in Seattle, in response to exercise intelligence citing a possible terrorist attack at the Columbia

³³ Homeland Security Presidential Directive/HSPD-5, February 28, 2003.

³⁴ T2 did not exercise the draft National Response Plan.

³⁵ United States Government National Response Plan (draft)
http://www.nemaweb.org/docs/National_Response_Plan.pdf

³⁶ Ibid.

³⁷ Ibid.

Generating Station near Richland, Washington.³⁸ Mr. Byrne was notified of the proposed diversion of the DEST from Richland to Seattle on May 12, 2003, at 1235, and he arrived at the Joint Operations Center (JOC) in the FBI Field Office in Seattle at approximately 1700. At the JOC, he worked closely with the Federal Emergency Management Agency (FEMA) Region X Director, senior DOE officials, and the FBI SAC.

Upon arrival, Mr. Byrne established a unified command where all Federal agencies with jurisdictional authorities contributed to the process of determining overall incident objectives, selecting strategies, ensuring integrated operations, and maximizing use of all resources. To ensure that the federal response was coordinated and that action plans were consolidated, Mr. Byrne led regular briefings with his Command Group, consisting of the DEST and liaisons from key Federal, State, and local jurisdictions and agencies. These briefings focused on the status of the response, assets deployed, consensus building, and the development of recommendations to present to the State and local authorities.

Mr. Byrne also directed that all federal communications would be integrated so that there was one consistent voice speaking for the Federal Government. In addition, he worked to ensure that the integrated federal communications was consistent with communications coming from the State and local authorities. He instructed the FBI JOC to be more forthcoming with information to both State and local authorities and with the JOC Consequence Management Group (CMG). Mr. Byrne also initiated and led regular conference calls with top officials (or their representatives) from Seattle, King County, Washington State, and FEMA. In these conference calls, he discussed current federal support, offered recommendations, responded to questions concerning issues raised by the State, county, and city officials, and tried to assure Seattle, King County, and Washington State officials that they had the same information that he had.

He was also concerned about the apparent lack of integrated communications prior to his arrival between the Joint Information Center (JIC) and DHS and took steps to rectify the problem. For example, he discovered that DHS had raised the threat level to Red in seven cities, closed roads and airports, placed restrictions at border crossings *without a message ever coming to the Washington JIC or JOC*. To rectify the situation, he instructed the JIC to provide a liaison to the JOC CMG and to communicate more regularly with DHS.

Mr. Byrne also kept in touch with DHS Headquarters through regular conversations with the DHS CAT.

³⁸ From the U.S. Government Inter-agency Domestic Terrorism Concept of Operations Plan: "The DEST is a rapidly deployable, inter-agency team responsible for providing the FBI expert advice and support concerning the U.S. Government's capabilities in resolving the terrorist threat or incident. This includes crisis and consequence management assistance, technical or scientific advice and contingency planning guidance tailored to situations involving chemical, biological, or nuclear/radiological weapons." Note that the DEST is now a DHS-managed asset that supports the Lead Federal Agency during a terrorist threat or incident.

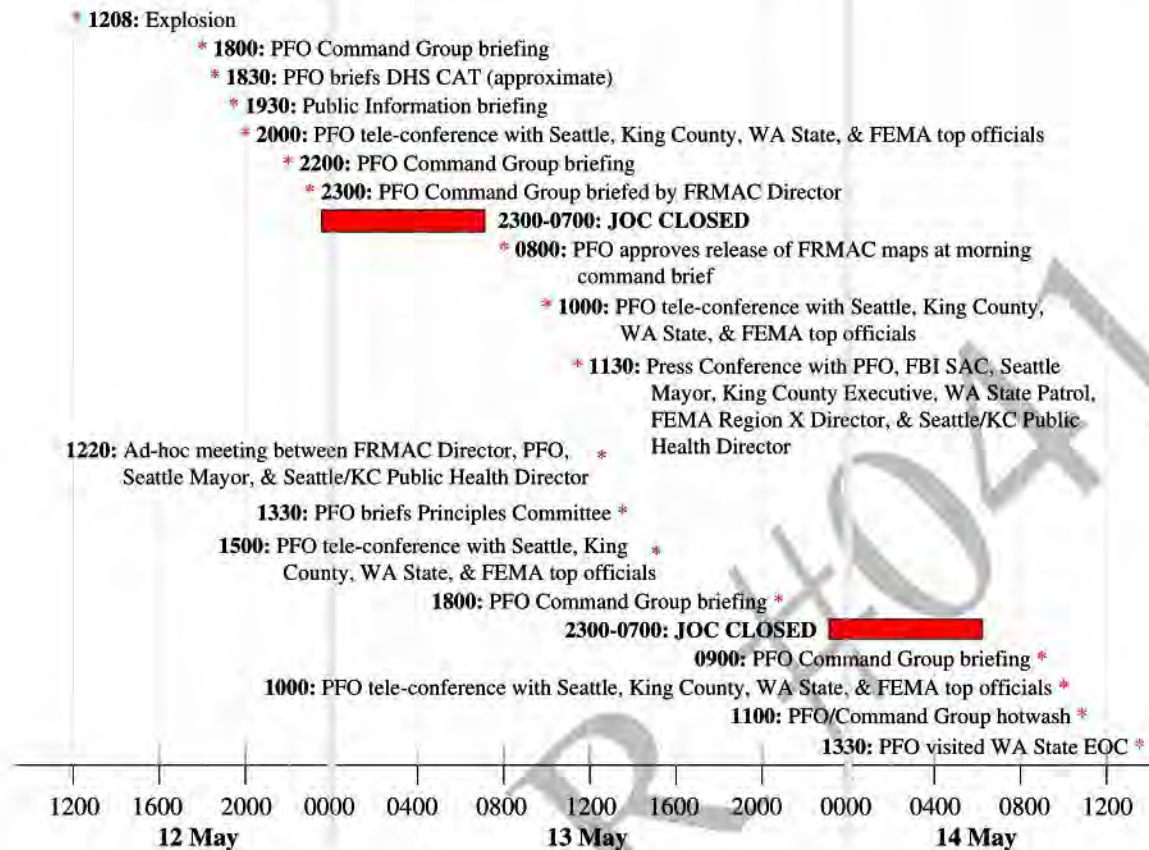


Figure 8. Outline of Principle Federal Official Key Events in Washington State (all times are Pacific Daylight Time)

b. Illinois

Wayne Parent, the Operations Coordinator for the Border and Transportation Security Directorate in DHS, was appointed the PFO in Illinois. In the Illinois venue, the PFO spent the first two days in the FEMA Regional Operations Center (ROC) and moved to the JOC when it stood up on May 14, 2003. At the ROC, he worked closely with the FEMA Region V Director. At the JOC, he worked with the Region Director (RD), the SAC, and the FCO.

As PFO, Mr. Parent ensured that communications were integrated, action planning between the SAC and the RD was coordinated, and that State and local officials that were actively involved. His approach was to foster consensus among the jurisdictions and agencies. To that end, a series of regularly scheduled teleconferences was held with Federal, State, and local (FSL) agencies. These calls featured briefings, coordination, de-confliction, and decision-making. Typically, Mr. Parent did not have to adjudicate among agencies; the teleconferences and follow-up discussions resulted in decisions reached through consensus.

Mr. Parent kept in touch with DHS headquarters through regular morning and evening conversations with the CAT leader. He also contacted the CAT leader when issues arose, with a total of four or five contacts per day. He provided an encapsulated situation report to the CAT during the evening conversation.

4. Artificialities

By design and consistent with the open book nature of the FSE, the PFO arrived in Chicago a week before the exercise and met in advance with many of the officials involved. In fact, HHS provided the PFO with a subject matter expert (SME) before he was officially appointed PFO. In addition, both PFOs had advance knowledge of the scenario. Thus, they had more situational awareness of the specific players and of the situations they would each be facing than a typical PFO would likely have in an actual incident. This is not a criticism of the PFOs; in fact, it likely enhanced the learning opportunity for DHS and all FSL agencies involved.

5. Analysis

a. The relationship between DHS and FEMA

The relationship between the PFO and the FEMA officials was different in the two venues. In Washington, Mr. Byrne's activities were consistent with his concept for the PFO role. This concept involved the development of a Command Cell, consisting of the PFO, FCO, FBI SAC, and State and local counterparts for the response phase of an incident. As envisioned, the PFO would prioritize and adjudicate between the often-competing needs of the crisis and consequence management sides of the response phase. This allowed the FBI SAC and the FCO to concentrate completely on their respective aspects of the response. Under this concept, the PFO truly became the one voice for the federal response. Mr. Byrne's view of the PFO role was clearly observed during the FSE. As PFO, he quickly instituted a unified command to manage the overall federal response and coordinate integrated communications and action planning, but left the FBI SAC to coordinate the crisis response, and left the FEMA RD and the FCO to coordinate the day-to-day activities of the federal consequence management assets.

It is important to remember that in Washington, although an RDD device was involved, the event unfolded in more of a traditional first responder fashion with a relatively well-delineated disaster site³⁹. With the rapid discovery of radiation, federal assets quickly came into the exercise picture and, importantly, a JOC was quickly established. In Illinois, events unfolded more gradually as would be expected during a disease outbreak. There were no clearly defined disaster sites (although release sites were eventually identified) and the JOC stood up a couple of days into the event. Mr. Parent worked within the framework of a unified command to ensure that integrated communications were achieved and that action plans were coordinated, but did so in a less overt manner than Mr. Byrne.

The different approaches to the role of the PFO suggest that DHS should take this opportunity to clearly de-conflict and define the responsibilities of the PFO with respect to the FEMA RD and FCO in the final NRP. The relationship may differ depending on the circumstances, but general guidelines need to be formulated and implemented. In addition, the PFO roles and responsibilities defined in the draft NRP may or may not be appropriate during the recovery phase of disasters. Since the recovery phase was not examined in much detail during the FSE, further exercises will be needed to shed some light on this issue.

³⁹ The uncertainties that responders faced at the RDD incident site are discussed in detail in the *Special Topics* sections: "Data Collection and Coordination: RDD Plume Modeling and Deposition Assessment" and "Balancing the Safety of First Responders and the Rescue of Victims."

b. PFO Resources

During the FSE, both PFOs required additional technical support beyond their administrative and security details to accomplish their respective roles and responsibilities. In Washington, Mr. Byrne used the DEST and, in some cases, the JOC CMG to support his efforts. He informed the evaluation team that the DEST has the capability to support the PFO, FCO, and FBI SAC during the response phase of an emergency if they are all co-located as a Command Cell. This has the added benefit of reducing redundancy, as Emergency Support Function personnel would not be needed to staff both the JOC CMG and the FEMA ROC.

In Illinois, Mr. Parent was provided with an SME from HHS after a meeting with the head of the HHS Secretary's Emergency Response Team (SERT). Mr. Parent reported to the evaluation team that this support was essential to helping him understand the specifics of the bioterrorism event and the critical role that HHS would play in a real-world event.

6. Conclusion

The FSE presented DHS with an excellent opportunity to evaluate and exercise emergency response procedures, teams, and assets. During the FSE, both PFOs encouraged and facilitated integrated communications and coordinated action planning. They also both encouraged active communication with State and local authorities. While their leadership styles may have differed, the roles that each PFO had during the FSE may have also reflected, to a degree, differences in the problems that each encountered and that the terrorist attacks developed differently in the two venues.

While the concept of the PFO was well-received, the roles and responsibilities of the PFO compared to those of the FEMA RD, the FEMA FCO, and the FBI SAC still need to be clarified. In addition, the PFO requires a staff with the flexibility and expertise to support all emergencies, natural and terrorist-related. If the DEST is expected to support the PFO and the Federal response, DHS should consider providing enough resources to staff at least one additional team in the event that more than one federal emergency occurs at the same time, as was exercised in the T2 FSE.

SUMMARY OF CONCLUSIONS— PFO:

The PFO was well received by Federal, State, and local authorities during the T2 FSE.

The roles and responsibilities of the PFO vice the FEMA FCO, FEMA Region Director, and FBI SAC need to be further clarified in the final National Response Plan.

The PFO requires a dedicated staff with the flexibility and expertise to support all emergencies.

D. Data Collection and Coordination: Radiological Dispersal Device Plume Modeling and Deposition Assessment In Washington

1. Introduction

During the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE), designers simulated the explosion of a radiological dispersal device (RDD) in Seattle, Washington. In the aftermath of an RDD explosion, the development of analysis products, including plume prediction models and radiological deposition maps, which show the potential impact of the radiation on people, agriculture, and the environment, is vital. These maps provide policy-makers and top officials with the information they need to make effective decisions.



In the initial hours following an RDD explosion, radiation experts rely on predictive plume models to give decision-makers a rough sense of how current weather conditions affect where the radioactive materials are likely to spread. As responders learn more information about the explosion—such as an estimate of the amount of explosives and the type(s) of radiological material used—additional data can be entered into the predictive plume models. Model outputs can then be used to update the prediction maps. During the FSE, different agencies and jurisdictions used one or more plume models to generate predictions, which led to both confusion and frustration among top officials in Washington State and Washington, D.C.

As the response progresses and empirical data are collected in the field, deposition or “footprint” data products are developed. For these products to be useful to decision-makers, subject matter experts (SMEs) must first interpret the data to determine the impact on people, agriculture, and the environment using Environmental Protection Agency (EPA) Protective Action Guidelines (PAG).⁴⁰

All radiological data collected by Federal, State, and local (FSL) agencies should be coordinated so that SMEs can develop the most up-to-date data products, and top officials in different locations have consistent information upon which to base their decisions. For Federal agencies, the Federal Radiological Emergency Response Plan (FRERP)⁴¹ assigns data coordination to the Federal Radiological Monitoring and Assessment Center (FRMAC). During the T2 FSE, however, coordinating data collection proved to be a significant challenge. As a result, FSL agencies that developed data products and deposition maps used different and incomplete data. A further challenge during the FSE was the distribution of the many data products generated throughout the exercise. In addition, confusion was apparent over the differences between maps

⁴⁰ EPA is assigned the responsibility for developing Protective Action Guidelines (PAGs) under various authorities, including the Radiological Emergency Planning and Preparedness Regulation (44 CFR 351). EPA coordinates the interagency development of the PAGs through a subcommittee of the Federal Radiological Preparedness Coordinating Committee.

⁴¹ The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.

generated from predictive plume models vice empirical data products and deposition maps. The impact on top officials was delayed decision-making or, in some cases, policy decisions that were made under conditions of uncertainty. Although decision-making under rapidly changing and ambiguous situations is always part of emergency response, overcoming the data coordination and analysis product distribution challenges can reduce the uncertainty observed during the FSE.

Two critical issues had a significant impact on the response observed during the T2 FSE:

- Coordinating the data collected by multiple agencies at FSL levels of government; and
- Developing and distributing analysis products—including plume model prediction overlays and empirical deposition, footprint maps—to subject matter experts (SMEs) and decision-makers by multiple FSL agencies.

In real emergencies and during the FSE, these two issues interact to impact decision-makers. Figure 9 shows what might be considered an ideal picture of the data collection, coordination, and product distribution process. Under most circumstances, data collection will take place in multiple locations and involve multiple agencies. The challenge is for all of these agencies to coordinate their data collection efforts and send all of the data to an agreed upon clearinghouse where it is interpreted, entered into a prediction model or developed into deposition maps, and then provided to SMEs and decision-makers. Again, for Federal agencies, this is the responsibility of the FRMAC as described in the FRERP.

However, if FSL agencies send their raw data to different locations, rather than a centralized location, and there is no coordination among the different agencies, then analysis will not be conducted with the complete data set. If the analysis and the resulting analysis products are not consistent, then top officials and policy-makers will have differing, and potentially conflicting, information. Such conflicts will impact officials' ability to develop consistent and agreed upon decisions. Follow-on legal implications and negative public perception are also potential results of a poorly-coordinated FSL response.

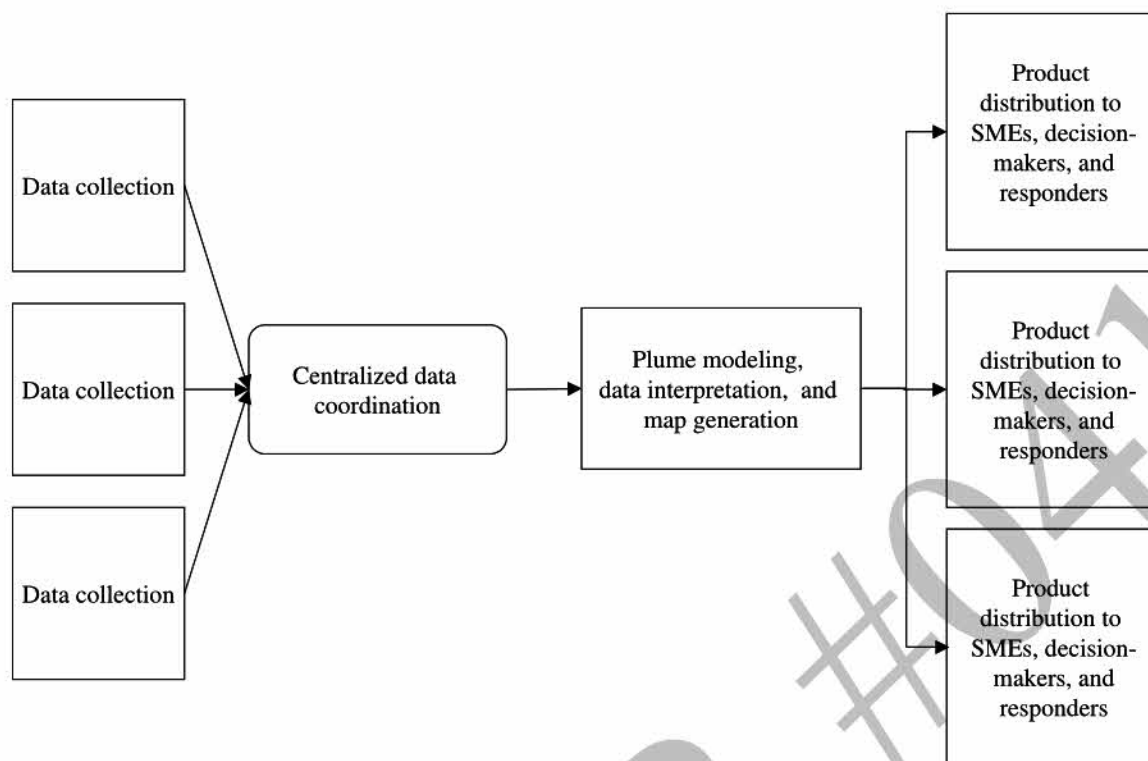


Figure 9. An Ideal Picture of the Data Collection, Coordination, Interpretation, and Dissemination Process

This special topic begins with a discussion of the FSL agencies and departments that have responsibilities or authorities under current FSL codes and inter-agency agreements to collect and coordinate radiological data; conduct analyses; and provide models, maps, and other analytic products in radiological emergencies. This background information is followed by a reconstruction of the events that occurred during the FSE and an analysis of the reconstruction. Finally, the last section contains conclusions based upon the analysis of the FSE and the existing codes and authorities.

2. Background

In the aftermath of an explosion containing radioactive materials, the detection of radioactivity will lead to a number of agencies being called to the scene. Some states, including Washington, have robust radiological incident management capabilities, and, therefore, provide State-owned assets to the incident. In addition, they can draw upon Federal assets from the Department of Energy (DOE), Environmental Protection Agency (EPA), Department of Health and Human Services (HHS), United States Department of Agriculture (USDA), the Nuclear Regulatory Commission (NRC), and others to augment their efforts.

Although capabilities for radiological detection across the United States and territories vary, the issues that arose during T2 are likely too generalized for many localities across the country. Therefore, it is useful to understand Seattle and Washington radiological detection capabilities and how their terrorism response plans are designed to integrate resources to create a unified

response. A discussion of the primary federal assets that have radiological response capabilities, focusing on agencies and departments that participated in T2, is also included.⁴²

a. City and state response capabilities

Seattle capabilities

Seattle Fire Department (SFD) Hazardous Materials (HAZMAT) vehicles and equipment have dosimeters that detect radiation. SFD HAZMAT personnel are likely to be the first radiation data collectors to arrive at a scene with suspected radioactive materials.⁴³

Washington State capabilities

- *Washington State Department of Health:*

In the Division of Environmental Health Programs, the Washington State Department of Health (DOH) maintains a Division of Radiation Protection. The division includes expert handlers of radioactive materials and incident management. DOH field team coordination is conducted from the Radiation Monitoring and Assessment Center (RMAC). The RMAC has the capability to provide dose assessment for field teams, collect and coordinate radiological data, and develop protective action recommendations and sampling plans⁴⁴.

In the event of a radiological incident, the Washington State DOH Public Health Laboratory supports the efforts of the Division of Radiation Protection to determine the immediate health risk to the public. The mission of the laboratory is to provide information to health officials as quickly as possible so that they have the data they need to assess the level of hazard to the public. The Radiation Chemistry Group rapidly performs radiological analyses to determine what radioactive materials are present in samples collected at an emergency site and can detect activity levels relevant to protective action guidelines⁴⁵.

- *Washington State Department of Ecology:*

Under the Spill Response Section in the Spill Prevention, Preparedness, and Response Program, the Washington State Department of Ecology maintains the Ecology Spill Response Team. While DOH has the overall authority in Washington State for radiological incidents, the Department of Ecology is often called upon for assistance since the Ecology Spill Response

⁴² The evaluation team is unaware of any King County radiological data collection teams or formal modeling capabilities at the King County EOC.

⁴³ There are nationwide efforts to increase the percentage of US jurisdictions with radiological detection capabilities. In July 2002, the U.S. Departments of Energy and Justice co-sponsored the Homeland Defense Equipment Reuse program (HDER). HDER provides surplus instrumentation and equipment to State and local fire, police and other emergency agencies to enhance their domestic preparedness capabilities. In FY 2003, deliveries to the pilot program cities included shipments to Philadelphia, Washington DC, Chicago, Detroit, Houston, Los Angeles, and San Francisco. In June 2003, the program was scheduled to go nationwide allowing all US states, the District of Columbia, Puerto Rico and the four US Territories to participate in the program and receive equipment, training, and local long-term technical support.

⁴⁴ Washington State Department of Health, Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack, DOH/DRP, March 2003.

⁴⁵ Information obtained from personal communication with DOH Public Health Laboratory personnel.

Team carries radiological monitoring instrumentation in all of their HAZMAT response vehicles⁴⁶.

- *National Guard Weapons of Mass Destruction-Civil Support Teams:*

The Civil Support Teams (CSTs) are congressionally-mandated units of the National Guard whose mission is to support State and local authorities at a domestic weapons of mass destruction (WMD) incident site. The CST supports civilian authorities by identifying WMD agents, advising for response measures, short- and long-term consequences, and facilitating the request of additional resources. The CST is a State-owned asset that can deploy without a Department of Defense (DOD) authorization. The Adjutant General can deploy the CST to support the state's response or to support another state's response if requested by that state's governor.⁴⁷

The CSTs are equipped with military standard radiation detection equipment. The survey team is also equipped with a handheld gamma spectrometer that provides the capability to identify specific gamma-emitting isotopes. The CSTs also have the capability to deploy with a mobile analytical laboratory system (MALS) to conduct on-site radiological isotope analyses.⁴⁸

b. Federal response capabilities and assets

Department of Energy

The National Nuclear Security Administration (NNSA) administers the many DOE assets that can be activated to respond to a radiological incident. These include:

- *Radiological Assistance Program:*

In the event of a radiological incident, the Radiological Assistance Program (RAP) provides radiological assistance when requested by other Federal agencies, states, local, or tribal authorities. A request for assistance normally comes first into one of eight DOE regional coordinating offices, specifically the Regional Response Coordinator (RRC). The initial response is typically a regional team of specifically trained personnel and resources that support the local authorities. The RRC has the authority to request one or more of the DOE assets (e.g., Atmospheric Release Advisory Capability, Aerial Measuring System, FRMAC, Radiation Emergency Assistance Center/Training Site, and other RAP regions) to support the response and to facilitate coordination between the DOE assets and other responding agencies.⁴⁹

- *Federal Radiological Monitoring and Assessment Center:*

According to the FRERP,⁵⁰ DOE is responsible for setting up and coordinating a FRMAC during the crisis phase of any radiological incident. Specific procedures are used to collect, analyze, assess, and disseminate data products useful to decision-makers. The efforts of all FRMAC

⁴⁶ Information obtained from personal communication with Washington Department of Ecology personnel.

⁴⁷ In Washington the commanding officer of the WMD-CST has the authority to self deploy his unit.

⁴⁸ This information was obtained from communication with LTC Thomas Hook, Army National Guard, Chief, Civil Support Team Program, National Guard Bureau Homeland Defense Division.

⁴⁹ Department of Energy, *Radiological Assistance Program*, (DOE 5530.3). Other information found at <http://www.doe.bnl.gov/RAP/rap.htm>.

⁵⁰ The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.

members are coordinated through these procedures to maximize efficiency and minimize confusion in their advice to decision-makers. Without such a coordinated effort, conflicting data products and excessively technical information may complicate decision-making. Once the FRMAC is established, all activated Federal assets are incorporated, and State and local technical experts are invited to co-locate and provide support to the FRMAC. Following the emergency phase, at a mutually agreeable time corresponding to the requirements found in the FRERP, the NNSA will transfer the responsibility of coordinating the FRMAC to the EPA. However, the NNSA and other federal agencies continue to support and provide resources to the FRMAC.⁵¹

The FRERP also calls for the establishment of the Advisory Team for Environment, Food, and Health (Advisory Team, or A-Team), which, while not a DOE asset, is co-located with the FRMAC. The A-team includes representatives from multiple Federal agencies and departments, including the EPA, USDA, HHS, and other Federal agencies, as warranted by the circumstances of the emergency. The A-team's primary responsibility is to provide the lead Federal agency (LFA) with advice on environment, food, health, and safety issues that arise during and from the emergency. The A-team provides direct support to the LFA but does not have independent authority.⁵²

- *Atmospheric Release Advisory Capability:*

Through the Atmospheric Release Advisory Capability (ARAC) program the DOE maintains the National Atmospheric Release Advisory Center (NARAC) at Lawrence Livermore National Laboratory (LLNL). NARAC provides atmospheric plume modeling tools and services for chemical, biological, radiological, and nuclear airborne hazards (both gases and particles) using real-time access to worldwide meteorological observations and forecasts through redundant communications links to data provided by the National Oceanic and Atmospheric Administration (NOAA), the U.S. Navy, and the U.S. Air Force. NARAC supports the Nuclear Incident Response Teams, the regional RAP teams, the Aerial Measuring System (AMS), the FRMAC, DHS under a DOE-DHS Memorandum of Agreement, and 40 DOE and DOD on-line sites. NARAC operational support of five cities and 53 state and Federal organizations across the country has been successfully tested under DHS and DOE support. NARAC can simulate downwind effects from a variety of scenarios, including fires, radiation dispersal device explosions, HAZMAT spills, sprayers, nuclear power plant accidents, and nuclear detonations. The NARAC software tools include stand-alone local plume modeling tools for end user's computers, and Web- and Internet-based software to reach-back to advanced modeling tools and expert analysis from the national center at LLNL. Initial automated, advanced 3-D predictions of plume exposure limits and protective action guidelines for emergency responders and managers are available in five to ten minutes. These can be followed immediately by more detailed analyses by 24/7 on-duty or on-call NARAC staff. NARAC continues to refine calculations as measurements are taken, until all airborne releases have stopped, and until the hazardous threats are mapped and impacts assessed. Model predictions included the 3-D and time-varying effects of weather and terrain. NARAC provides a simple Geographical Information System (GIS) for display of plume predictions with affected population counts and detailed maps, in addition to

⁵¹ Department of Energy, *FRMAC Operations Manual Emergency Phase*, (DOE/NV 11718-080 UC-707), May 1997. Other information found at <http://www.nv.doe.gov/programs/frmac/default.htm>.

⁵² The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.

the ability to export plume predictions to other standard GIS systems. NARAC products can be distributed through a password-controlled and encrypted website, e-mail or fax.

The Environmental Protection Agency

The EPA responds to radiological incidents under both the National Oil & Hazardous Substances Pollution Contingency Plan (NCP) and the FRERP. EPA can serve as the LFA, or can support State and local governments and the lead Federal agency by:

- Conducting environmental monitoring, sampling, and data analysis;
- Assisting responders in ensuring protection of Health and Safety;
- Assessing the national impact of any release on public health and the environment through the Agency's Environmental Radiation Ambient Monitoring System;
- Providing technical advice on containment and cleanup of the radiological contamination; and
- Assisting in site restoration and recovery.⁵³

EPA's On-Scene Coordinators maintain emergency response readiness, including survey and sampling equipment, for chemical and radiological incidents. In addition to a region's response capability, EPA Headquarters can also deploy its Radiological Emergency Response Team (RERT) to the accident scene as part of its radiological response. EPA's RERT provides additional specialized monitoring, sampling, and both mobile and fixed laboratory capabilities. As part of the A-Team, EPA's RERT members can provide State and local authorities with advice on protecting local residents from exposure to elevated radiation levels. Once the FRERP is activated, EPA radiological assets are expected to integrate with the FRMAC.^{54,55}

c. Requesting federal assets

State and local governments, as well as tribal governments and private organizations, can request support from a number of Federal assets to support their response and recovery efforts following an explosion that includes radioactive materials. For example, the EPA receives their authority to respond to any release of a hazardous substance from the National Oil and Hazardous Substance Pollution Contingency Plan (National Contingency Plan)⁵⁶ and the Public Health Services Act, among others. The DOE has similar authority to respond to a radiological incident as outlined in DOE 5530.3⁵⁷ to be superseded by DOE O 151.1A.⁵⁸

⁵³ Environmental Protection Agency, *Radiological Emergency Response Plan*, January 2000. More information found at <http://www.epa.gov/radiation/rert/index.html>.

⁵⁴ EPA's regional responders provided support to the local Incident Command System during the FSE. In addition, EPA deployed the Advance Units of its RERT. However, given the limited timeframe of the exercise and limited funding, EPA did not deploy RERT members who would have realistically only been able to arrive at the incident scene as the exercise drew to a close.

⁵⁵ Information specific to the EPA RERT is found at <http://www.epa.gov/radiation/rert/rert.htm>.

⁵⁶ Title 40 Code of Federal Regulation (CFR) 300, National Oil and Hazardous Substance Pollution Contingency Plan.

⁵⁷ Department of Energy, *Radiological Assistance Program*, (DOE 5530.3). Other information found at <http://www.doe.bnl.gov/RAP/rap.htm>.

⁵⁸ Department of Energy, *Comprehensive Emergency Management System*, (DOE O 151.1A).

In combining the responsibilities and authorities defined in the FRERP,⁵⁹ Concept of Operations plan (CONPLAN),⁶⁰ HSPD-5,⁶¹ and the Federal Response Plan,⁶² the following command and control functions—relevant to data coordination and plume modeling—were followed for Federal agencies during the FSE:

- DHS was designated the LFA, and coordinated the response from all Federal agencies; and
- DOE and EPA were technical support agencies to the LFA for the radiological aspect of the response; DOE was further responsible for coordinating the activities of the FRMAC.

d. Coordinating the data

There are many responders that can collect on-site and off-site radiological data following an explosion containing radioactive materials. To develop reliable (i.e., consistent) and valid information for decision-makers, it is important that the data collection effort be coordinated both on the ground and in terms of how the data flows and is turned into useful information for decision-makers. Coordinating the data flow can ensure that SMEs have all of the available data to use for analysis. This is one step to ensuring that the output—the information provided to policy makers and top officials—is consistent and valid in terms of the empirical data. Coordination on the ground also helps to minimize the likelihood that multiple agencies will perform redundant tasks or repeat tasks because of conflicting data reports. This is vitally important in an incident where responders face a high-risk environment.

The Washington State DOH Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack describes how the DOH should coordinate their radiological response on-site and with the FRMAC. Prior to the arrival of the FRMAC, the State Health Liaison (SHL) facilitates communication between the DOH staff at the Washington State Emergency Operations Center (EOC) and incident command regarding appropriate protective measures and decisions. The SHL provides the WA State EOC with radioactive release data, weather data, radiological data collected by field teams, predictive plume maps, and dose projections. Once the FRMAC is established, the SHL or Deputy State Health Liaison (DSHL) relocates to the FRMAC and assumes the role of FRMAC liaison. The WA State DOH response plan leaves the details of the coordination effort up to the SHL (or DSHL) and the FRMAC, which provides for the flexibility needed for each individual response. The FRMAC liaison is responsible for coordinating the State's response with the Federal response and for maintaining communication with the FRMAC, the WA State EOC, and the Joint Information Center (JIC). Furthermore, the FRMAC liaison is responsible for determining when and how Washington State's response will be integrated with the Federal response.⁶³

Typically, upon arrival at a crisis, the FRMAC Director works to coordinate with State and local agencies through an advance party meeting. The goals of the advance party meeting are to ensure that Federal representatives in the FRMAC are up-to-date on the crisis, identify points of

⁵⁹ The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.

⁶⁰ United States Government Interagency Domestic Terrorism Concept of Operations Plan.

⁶¹ Homeland Security Presidential Directive/HSPD-5, February 28, 2003.

⁶² Federal Emergency Management Agency, *Interim Federal Response Plan*, January 2003 (9230.1-PL).

⁶³ Washington State Department of Health, *Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack*, DOH/DRP, March 2003.

contact for state representatives, and develop protocols for providing data products to top officials and SMEs at state and local EOCs and relevant agencies. The advance party meeting is a critical step providing unique information during each emergency—different states have different relationships with county and local governments; the FRMAC representatives need to understand these relationships to provide effective support. The Federal response effort relies on state representatives to help facilitate these relationships. State and local radiation experts are also invited into the FRMAC to provide a liaison between the Federal response assets and the state and local governments. By having state, and potentially local, representation at the FRMAC, local decision-makers are still relying on their own people for recommendations. These SMEs, however, have additional support from the Federal Government.^{64,65}

e. Plume Modeling and Deposition Maps

In an RDD explosion, the bomb throws radioactive material into the air; the resulting radioactive debris cloud is called a plume. In the early hours following the explosion, the National Atmospheric Release Advisory Center (NARAC), the National Oceanic and Atmospheric Administration (NOAA), and the Defense Threat Reduction Agency (DTRA) can generate a prediction of the plume boundaries using sophisticated models. There are also several less sophisticated models available to develop a plume projection. To generate predictions, agencies need some basic information about the explosion and the radiological material involved (defined as the source term), the weather, and the topography surrounding the incident site. As more information about the explosion becomes available, the source term and the initial prediction are refined. Top officials can use these predictions to make preliminary decisions involving first responder safety, safe transit routes, and protective action guidelines for the public. The first plume prediction generated for SFD on May 12, 2003 by the Lawrence Livermore Atmospheric Release Advisory Capability (ARAC) model overlaid on the map of the Seattle region affected by the RDD explosion is shown in Figure 10.⁶⁶

⁶⁴ The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.

⁶⁵ Information obtained from personal communication with FRMAC personnel.

⁶⁶ For a detailed discussion of plume dispersion models, see the *Stanford Report*, an appendix to Annex B.

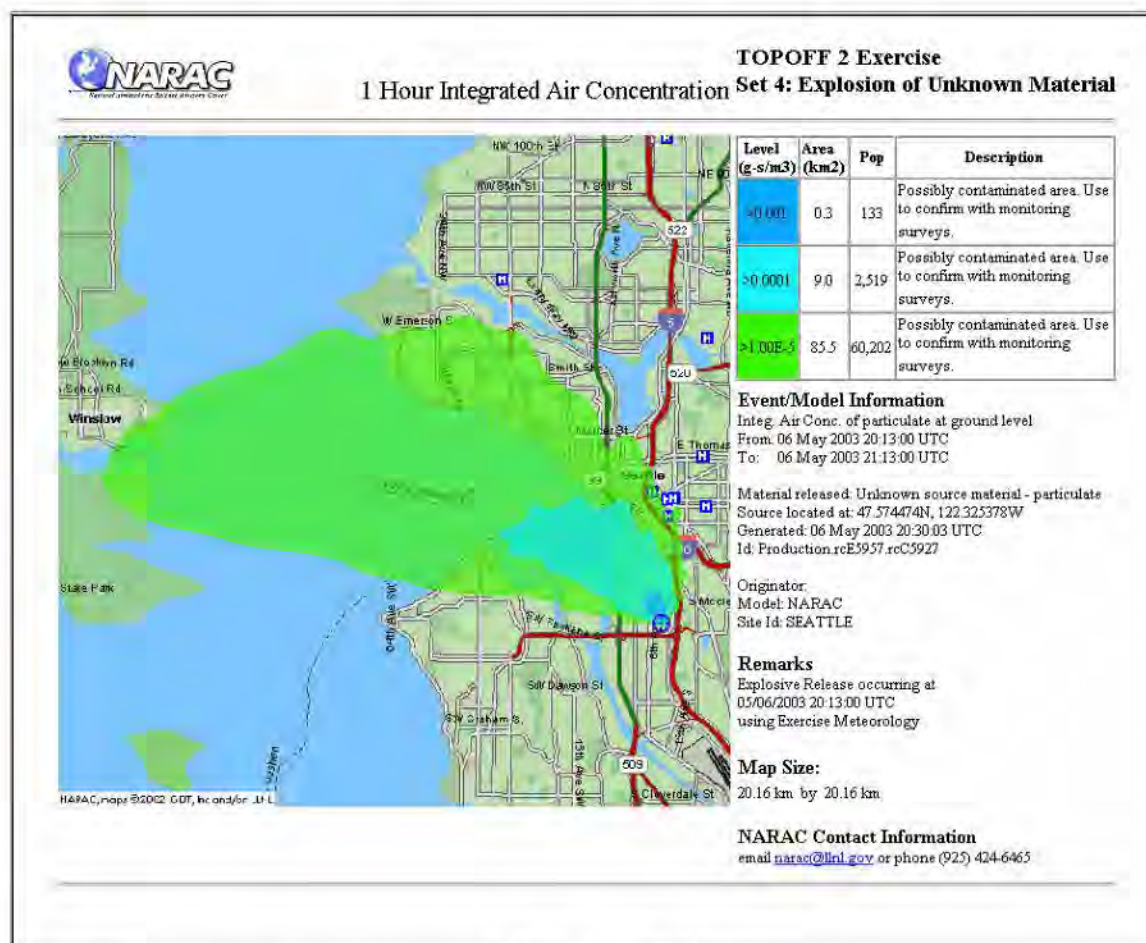


Figure 10. NARAC-Predicted Contaminated Areas

The plume predictions, alone, decrease in value after the first few hours following an RDD explosion. Knowledge about the type and amount of radionuclide released (as well as the physical form and chemical composition of the substance used) limit the modeler's ability to generate a plume prediction map that accurately reflects the release. The radioactive particulate matter that deposits on the surface during the passage of the plume can be measured by collecting empirical data with field-team and aircraft-based sensors. As more data are collected, a more accurate picture of the amount of radiological material deposited is developed. Initial measurement data can be used to update model predictions and produce a better prediction for areas that have not yet been surveyed. (For example, this was done during the FSE in the FRMAC using NARAC models to project areas that may have had low levels of food crop contamination in western Washington State.) Predictions updated with measurement data can also be used to make estimates of areas that have contamination below the measurement threshold of available instruments. When detailed measurement surveys are completed and the data analyzed, they can be used to determine the most accurate picture of the amount of radioactive material deposited. With these data, accurate assessments of protective actions can be made and used by top officials to confidently make informed decisions.

To be useful in managing the safety of victims or responders, the numbers characterizing the deposition of radioactive material on the ground must be turned into numbers characterizing the

dosage that a human would receive, and of more importance to top officials, into characterizations of the health impact of such a dosage. Figure 11 is a FRMAC data product that shows the radiological deposition on May 14, 2003 in terms of EPA PAGs. This product was generated based on a FRMAC assessment of measurements of the deposited radioactivity, and used the NARAC model to determined EPA PAG levels in between measurement points.

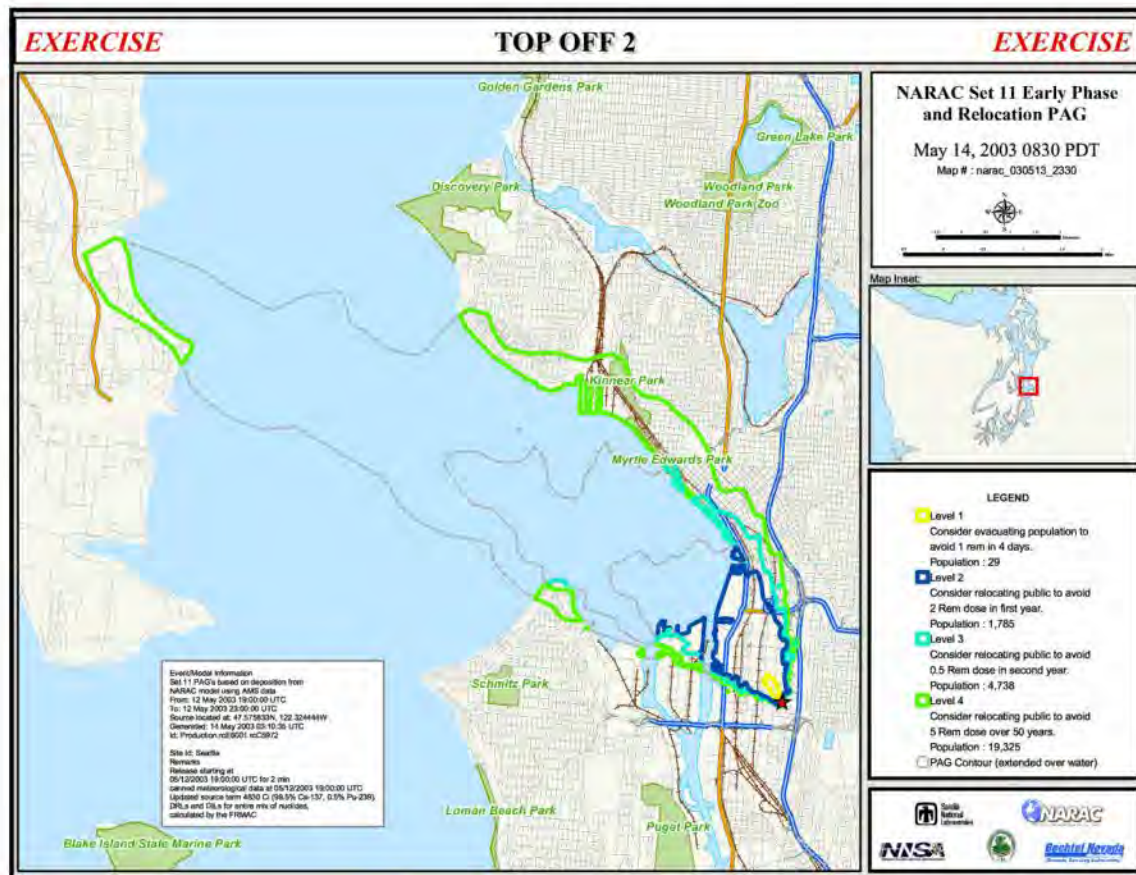


Figure 11. FRMAC Data Product Showing the Deposition of Radioactive Material in Terms of the Environmental Protection Agency's Protective Action Guidelines

Figure 12 describes the processes involved in developing plume predictions and deposition data products. It also highlights the differences between plume predictions and deposition, footprint data products and what each can provide the decision-maker.

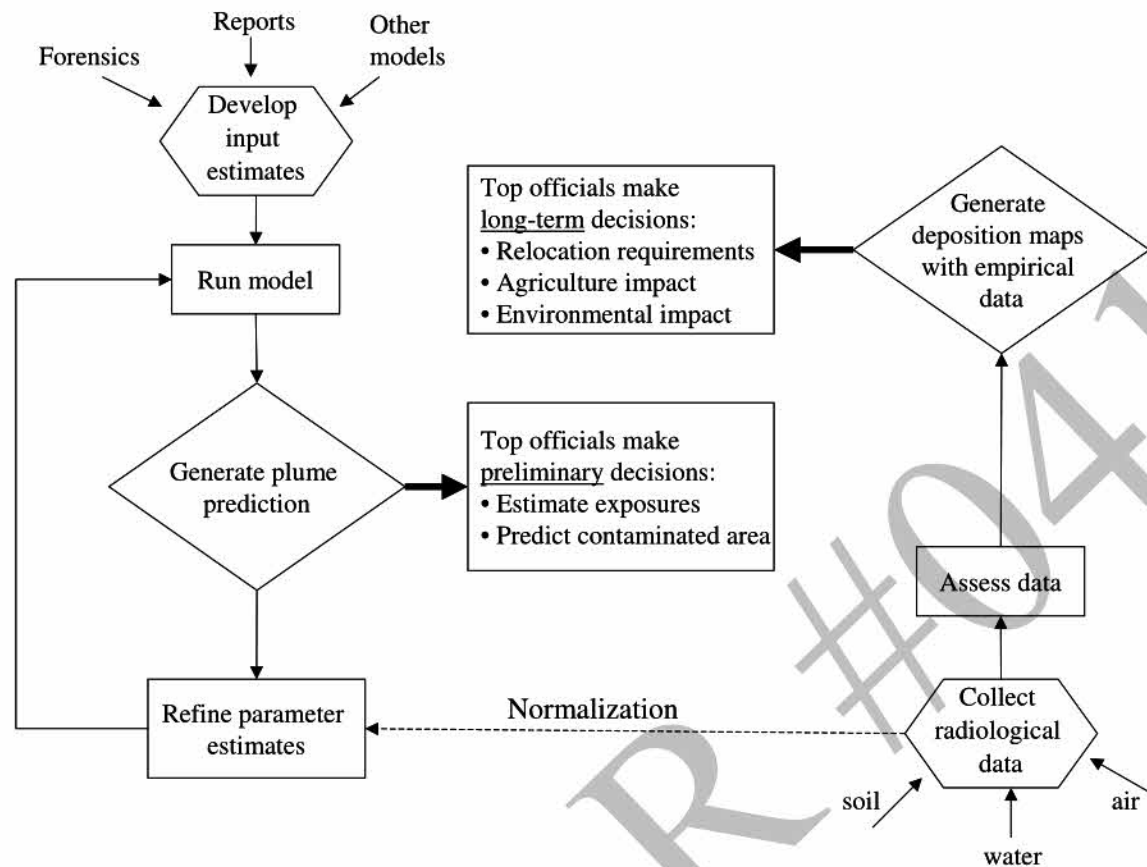


Figure 12. Processes for the Development of Plume Prediction and Deposition Maps

3. Reconstruction

The following teams all collected radiological data during the T2 FSE:⁶⁷

- City assets
 - Seattle Fire Department HAZMAT
- State assets
 - National Guard 10th WMD CST
 - Washington State DOH RMAC and Field Teams
 - Washington State Department of Ecology Field Team

⁶⁷ The evaluation team learned that the ATF Bomb Squad carried radiation detectors that they used to collect data for their personal use. It is possible that there were other agencies whose personnel were also wearing radiation detectors. US Navy personnel from the Puget Sound Naval Shipyard were also tasked during the FSE to collect radiological data for the FRMAC. It is possible that the evaluation team is unaware of other agencies that collected radiological data during the FSE.

- Federal assets
 - DOE RAP Region 8 Team
 - DOE Aerial Monitoring System (AMS)
 - EPA Field Team
 - FRMAC Field Teams

As shown in figure 13, no single agreed upon agency served as a central clearinghouse for all of the radiological data collected by the different teams. Data were collected and sent to multiple agencies for analysis, but no one agency received all of the data.

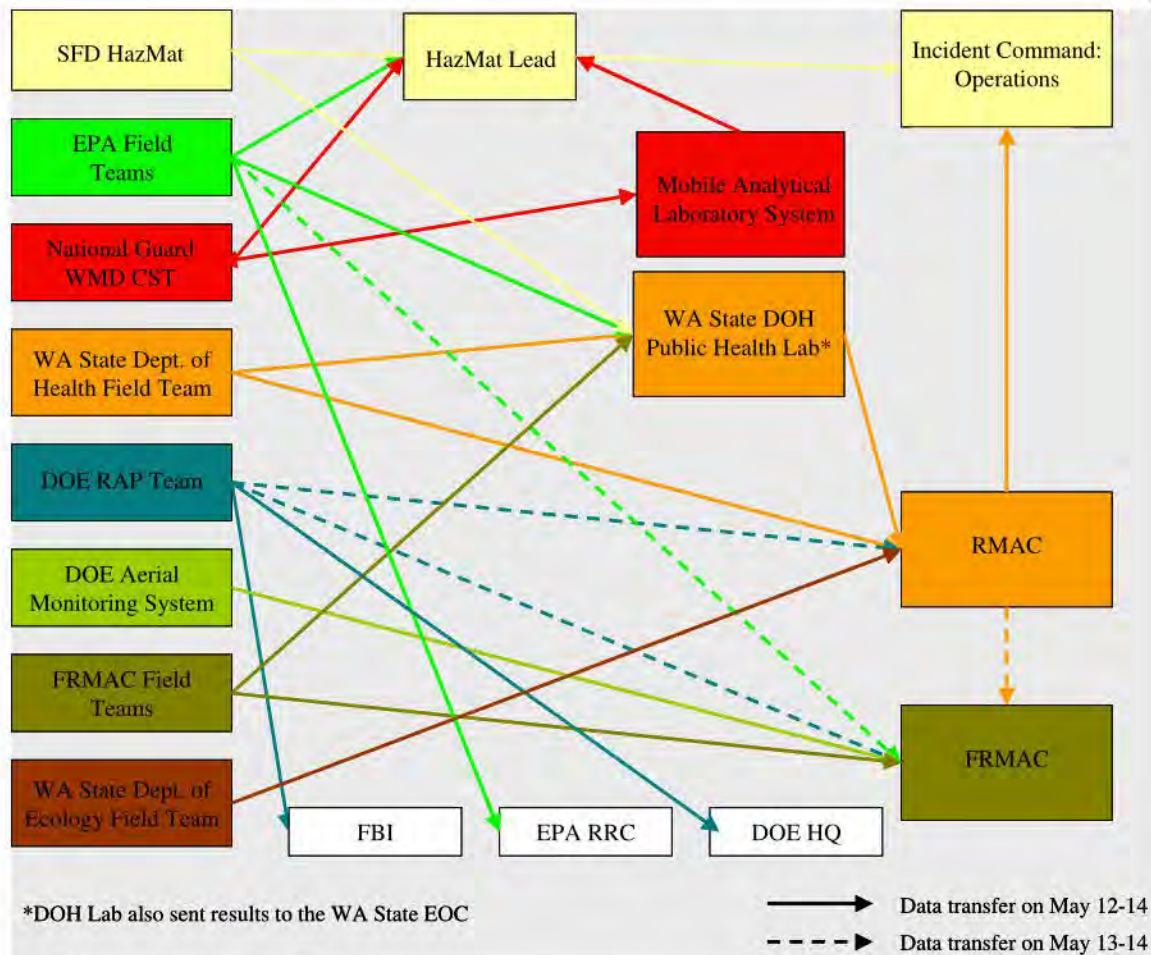


Figure 13. Data Coordination during T2 FSE

The following agencies/organizations generated and distributed plume predictions and/or deposition maps during the FSE:

- State and local
 - SFD/Seattle EOC
 - Seattle/King County Public Health EOC
 - King County EOC
 - Washington State DOH RMAC
- Federal
 - FRMAC
 - HHS Headquarters
 - NOAA
 - DOE Headquarters

Figure 14 indicates that many data products were produced by many different organizations. The distribution of these products also proved to be a challenge during the FSE.⁶⁸

⁶⁸ According to a Washington DOH controller after the FSE, data was sent from the RMAC to the Seattle EOC, but the evaluation team could not confirm that information.

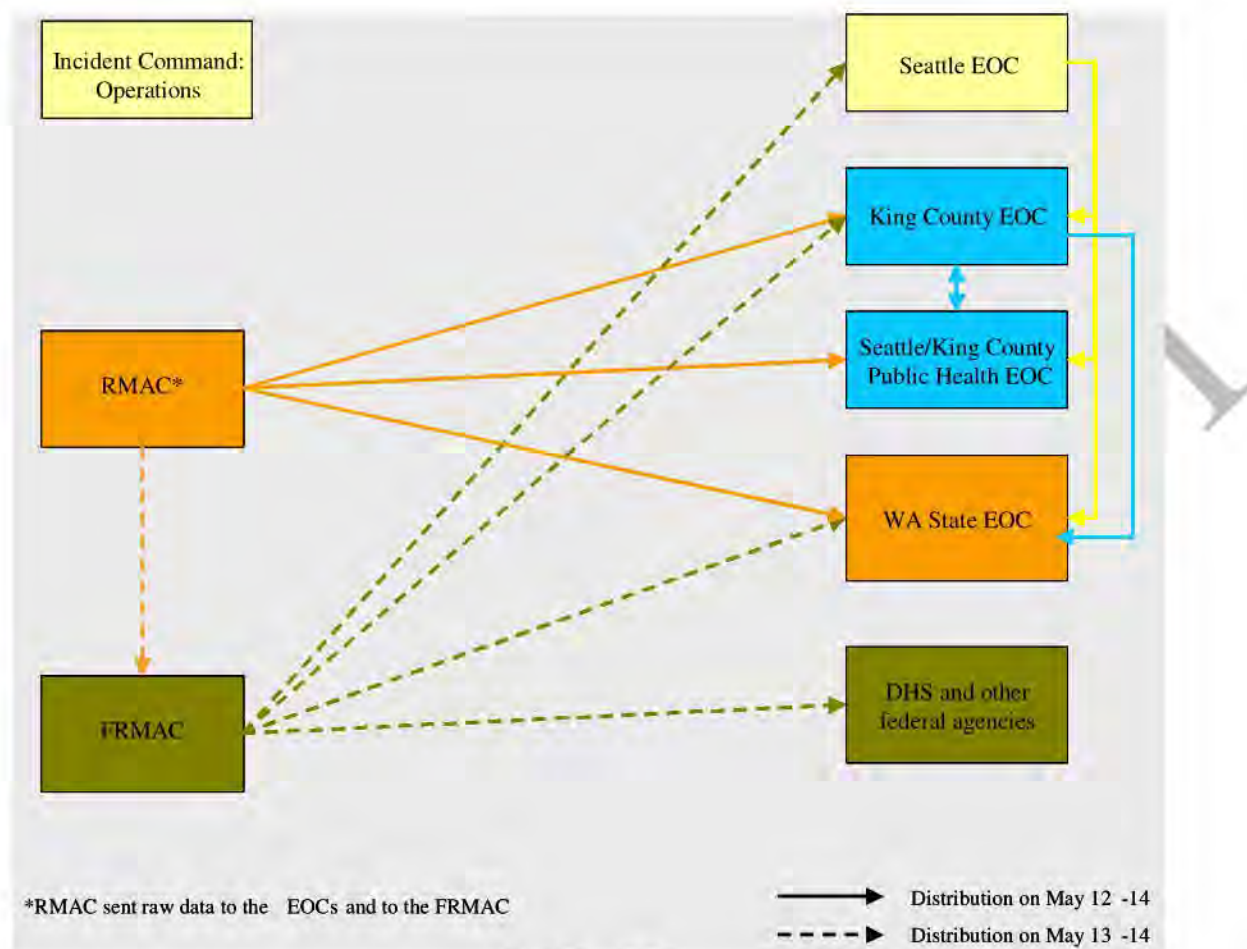


Figure 14. Data Interpretation and Distribution during T2 FSE

a. Seattle

Soon after the explosion, SFD generated a prediction of the plume using the ARAC model.⁶⁹ It is not clear, however, if the initial plume prediction generated by SFD ever left the incident site. All other plume predictions were generated by NARAC upon request and made available to agencies via the NARAC secure Internet site. Distribution of NARAC predictions to other agencies (beyond Seattle) required approval by the DOE Senior Energy Official, who was responsible for coordinating the use of DOE assets (such as NARAC) with other agencies. Agencies that had access to the NARAC secure Internet site included SFD, Seattle Police

⁶⁹ Seattle is the first city to pilot the Local Integration of NARAC with Cities (LINC) program. The program was a pilot project of the NNSA, and is now in DHS. It enables local responders to access NARAC's plume modeling capabilities. Using the system, the Seattle Fire Department (SFD) can receive NARAC plume model predictions using previously installed computer systems. The NARAC predictions can easily be distributed to multiple recipients. For more information, refer to *NNSA's Livermore Lab Partners With Cities and Counties to Track Biological, Chemical Releases*. Lawrence Livermore National Laboratory News Release, NR 02-05-08, May 22, 2002.

Department (SPD), Seattle EOC, Public Health Seattle/King County (PHSKC) EOC, King County EOC, WA State EOC, WA DOH, DHS, Federal Emergency Management Agency (FEMA), DOE, DOD, Department of Transportation (DOT), HHS, (NRC, and EPA.

b. Washington State

The Seattle EOC notified the WA State EOC that SFD responders detected radiation at the incident site at 1225 Pacific Daylight Time (PDT). The WA State EOC deployed the following assets:

RMAC

The WA State DOH deployed their mobile RMAC to the incident site shortly after the WA State EOC received notification that radiation was detected. By mid-afternoon on May 12, 2003, the RMAC gleaned enough information off the radio to develop a source term and generate its own plume projection using a modeling program called HotSpot. The RMAC also deployed field teams that were collecting data by 1530, and obtained off-site readings by 1900.⁷⁰

The RMAC had considerable communications problems throughout the exercise—that could have just as easily occurred in a real incident. During the afternoon and evening of May 12, 2003 and the morning on May 13, 2003, the RMAC was only able to transmit data points to the WA State DOH staff at the WA State EOC via telephone. Those data points were plotted on a map at the WA State EOC. The RMAC also used the EPA's wireless Internet capability to send graphics to the DOH staff. However, the file was not recognized as containing graphics and was not opened immediately. At 1455 on May 13, the RMAC used the DOE Region 8 RAP Team's fax machine to transmit three pages of field team data. Because of the lack of resources at the WA State EOC to plot data and the considerable lag time to receive data, the Division of Radiation Protection Director began identifying significant data points and briefing them directly to decision-makers during conference calls.⁷¹

The RMAC also sent data to the King County and PHSKC EOCs and to the FRMAC during the exercise. The DOH liaison at the King County EOC began sending a courier to the RMAC to pick up their radiation data on the morning of May 13, 2003. Plotters in the King County Geographic Information System (GIS) section then plotted the data points on a map and forwarded it to the WA DOH staff at the WA State EOC. The DOH liaison at the PHSKC EOC received data over the telephone and plotted it on a map. By late afternoon on May 13, a DOH liaison went to the FRMAC to initiate a protocol for transmission of data. Because of communications problems, the FRMAC did not begin to receive DOH RMAC data until May 14.⁷² The Seattle EOC does not recall ever receiving data or products from the RMAC or the WA State DOH.

DOH Public Health Laboratory

The DOH Public Health Laboratory was activated to analyze soil samples. They received soil samples from the DOH field teams, EPA field teams, and FRMAC field teams. To test their

⁷⁰ RMAC teams were likely on site earlier but there are no data to confirm this assertion.

⁷¹ The reconstruction of events at the DOH RMAC was obtained through conversations with Washington DOH staff who participated in the exercise.

⁷² Information regarding data transmission from the RMAC was reconstructed from conversations with Washington DOH and FRMAC staff who participated in the exercise.

internal policies and radiation analysis capabilities, the lab arranged to receive radioactive soil samples prepared prior to the FSE. For purposes of the exercise, these samples were tagged as though they came from SFD HAZMAT, EPA, and Harborview Hospital. The results were sent to the RMAC and to the WA State EOC.

Department of Ecology

At 2000 on May 12, the WA State EOC was prompted by exercise control to contact the Department of Ecology and have them deploy their HAZMAT team resources to survey the surrounding area. At 2312 a data collector observing incident command recorded the Operations Chief instructing the Ecology Field team to do off-site monitoring. The Ecology Field Team data were sent to the RMAC.

National Guard 10th WMD CST

The WA State EOC notified the National Guard 10th WMD CST to go on standby at 1230 on May 12, 2003. They were instructed to deploy to the City of Seatac and await further instructions. At 1345, the CST received notification from the WA State EOC to deploy to the incident site.⁷³ The CST advance team arrived at the incident site at approximately 1415, and the CST commanding officer met with the Incident Commander at 1420. The CST commanding officer was instructed to check in with the SFD Operations Chief and report directly to the HAZMAT Chief. After an initial assessment, the CST commanding officer brought in the rest of his team at 1445. The CST sent their data to the SFD HAZMAT Chief and to their MALs. They also collected ground samples that the EPA sent to the WA State DOH Public Health Laboratory for analysis. The CST was redeployed at approximately 1230 on May 13, 2003 and told to remain on stand-by in case there were follow-on attacks.

c. Federal data collection and modeling

The following Federal assets were deployed to Seattle and the surrounding areas:

EPA

At 1318 on May 12, 2003, EPA regional field personnel were dispatched to the incident site. When they arrived on scene, EPA personnel communicated with incident command and were tasked with monitoring the perimeter and taking air samples. EPA personnel began monitoring and sampling at approximately 1430; they continued to take air and soil samples throughout the exercise. EPA responders provided their data to incident command through the Incident Command System (ICS) reporting chain. EPA responders also provided data back to EPA Region 10 Regional Response Center (RRC). While EPA has procedures to provide off-site data to the FRMAC during a fixed-facility incident, procedures for integrating on-site data into the FRMAC were not been provided to the EPA field teams during the FSE.⁷⁴ As a result, while EPA personnel knew to send their data to the FRMAC, no data were sent to the FRMAC until May 14.

⁷³ The CST deployed to the exercise staging area prior to the start of the exercise. They waited there for the appropriate amount of time as if they were following the deployment orders described above.

⁷⁴ As will be discussed later in the section, EPA data was not provided to the FRMAC until May 14 because no advance party meeting was held during the FSE.

DOE Region 8 RAP Team

At 1335 and 1336 respectively on May 12, 2003, the Region 8 RAP received calls requesting assistance from the WA DOH and the Federal Bureau of Investigation (FBI). Within two hours, the team completed their pre-deployment activities and was en route to the Seattle area by 1458. Through discussions with both the FBI and WA DOH, it was agreed that RAP would initially put all their resources and effort to support the FBI. Upon arrival at the scene, RAP teamed up with the FBI Hazardous Material Response Unit (HMRU) Commander, informed him of team capabilities, and received a safety brief prior to commencing survey onsite. RAP supported the FBI until 2400 on May 12 and continued to support the FBI on May 13 until 1100. RAP received numerous requests for assistance from the Environmental Protection Agency (EPA), who were conducting on-site surveys, and the Disaster Mortuary Operational Response Team (DMORT). RAP fulfilled these requests and supported WA DOH with their requested priorities into the evening of May 13. On May 14, RAP was able to fulfill a request to join the FRMAC.

DOE AMS

A data collector at the WA State EOC recorded that the deployment order for the AMS was received at 1425 on May 12, 2003. The DOE AMS arrived over Seattle at approximately 1900 and flew a serpentine pattern to collect notional radiological data. The data were transmitted to the FRMAC at 2056. The AMS flew several more times over targeted locations during the FSE.

FRMAC

After some discussion among Washington State top officials concerning the need for the FRMAC, the DOH made a request to FEMA to deploy the FRMAC at 1434 on May 12, 2003. DOE Headquarters in Washington, D.C., approved the FRMAC deployment at 1549 that same day, and they departed from Nevada at 1600. At 2000 the WA State EOC received confirmation that the FRMAC was in place at Fort Lawton.

Upon establishment of the FRMAC, Field Monitoring Teams were deployed. At 2056 on May 12, 2003, the FRMAC began to receive simulated empirical aerial sampling data from the DOE AMS. The ground monitoring data obtained indicated the presence of an alpha emitter in addition to the gamma emitter identified earlier in the day.⁷⁵ With data still limited, the FRMAC Director briefed the initial results to the PFO at around 2300 on May 12 and recommended to the PFO that the affected people be evacuated. However, EPA advised the PFO that the Seattle Mayor's shelter-in-place order should not be revised, and that the decision could be re-examined in the morning based upon additional monitoring data. The PFO's final decision was to recommend to the Seattle EOC that they maintain the shelter-in-place until morning when a more thorough analysis would be completed. Before the PFO could pass his recommendation to the Seattle EOC, however, he learned that a decision had already been made by the Seattle Mayor to release those workers who had been sheltered within their businesses, and for residential citizens already sheltering-in-place to remain doing so.

The FRMAC did not have the time to complete a radiological deposition map that showed the health impact of the radiation dose on the public in terms of EPA PAGs before the Joint Operations Center (JOC) closed at 2300. FRMAC protocol required approval from the FRMAC

⁷⁵ Data collector logs show that the DOH Public Health Lab also identified the presence of an alpha emitter at around the same time.

Director, the Senior Energy Official (SEO), and the PFO—all of who were stationed in the JOC—before all analysis products could be distributed. Because the JOC was closed, the FRMAC could not obtain necessary approval to distribute the maps showing the radiological deposition to the other FSL operations centers until the following day.

At 0800 on May 13, 2003, FRMAC briefed the most up-to-date deposition map to the PFO. A more rigorous analysis revealed that an evacuation was not necessary, but a targeted relocation would be required. The PFO approved the release of the deposition map to the DHS Crisis Action Team (CAT). At 1000, FRMAC participated in a conference call with the PFO; the Seattle, King County, and WA State EOCs; and the FEMA Regional Operations Center (ROC). During that call, the FRMAC Director provided the EOC representatives with a summary of the data collected thus far. With this knowledge, in addition to the determination by WA DOH that the areas east of Interstate-5 (I-5) were contaminant-free, the Seattle Mayor was comfortable moving forward with his decision to release those residents sheltering-in-place east of I-5 and relocate affected residents west of I-5 for three days. Later that day, at 1220, the Seattle Mayor and the Public Health Seattle/King County Director met with the FRMAC Director and the PFO at the JOC to review the FRMAC deposition map.

After that meeting, the distribution of a consistent data product appeared to improve. Requests started to appear in the FRMAC activity log from the Seattle EOC and the WA State EOC for the most recent maps. The FRMAC responded to these requests anywhere from immediately (to DHS) to five hours, 38 minutes later (see Table 5). This timeframe provides a realistic sense of how long it takes for information to get out of the FRMAC once the contacts are established. Top officials and SMEs need to remember that the FRMAC is inputting data collected from many sources, and that before they distribute updated information, they need to input the data into their system, conduct an analysis of the data, and get approval from the appropriate authorities. This process takes time and is often shortened during training exercises.

Table 5. Request and Delivery of FRMAC Data Products

REQUESTING AGENCY	FRMAC PRODUCT REQUESTED	FRMAC PRODUCT DELIVERED	TIME DIFFERENCE
DHS	May 13 0851	May 13 0851	0:00
DOE Headquarters	May 13 0911	May 13 0920	0:09
FEMA ROC	May 13 0919	May 13 1239	3:20
DHS	May 13 0954	May 13 1359	4:05
Washington DOH	May 13 1137	May 13 1715	5:38
SFD	May 13 1143	May 13 1607	4:24
Seattle Mayor	May 13 1147	May 13 1402	2:15
Washington Department of Agriculture	May 13 1222	May 13 1735	5:12
WA State EOC	May 13 1318	May 13 1723	4:05
Food and Drug Administration	May 13 1901	May 13 2206	3:05
EPA	May 13 1909	May 13 2026	1:17
King County EOC	May 14 1055	May 14 1247	1:52

Many agencies and departments outside of Washington State contacted the FRMAC directly for maps and other data products on May 13 and 14, 2003. The FRMAC Event Log shows requests for deposition maps from DHS, Food and Drug Administration, EPA, and DOE Headquarters. These examples suggest that the Federal agencies participating in Washington, D.C., understood that the FRMAC would coordinate the radiation data and distribute the updated deposition maps. However, even though they had representatives in the A-Team—which was co-located with the FRMAC—deposition maps could not be sent to the Centers for Disease Control and Prevention (CDC) and the HHS operations centers.⁷⁶

d. Federal agencies and department headquarters

The following Federal agencies used their own internal models to develop maps at their headquarters:

DOE

DOE Headquarters in Washington, D.C., accessed the same NARAC plume predictions as those used by agencies working in the Seattle area (such as in the Seattle EOC and the FRMAC), using the same secure Internet site as used by other agencies. As DOE was assigned initial management of FRMAC for radiological response, it is likely that their plume map was used to brief top officials.

⁷⁶ The evaluation team does not know if this was because of technical problems or if the Advisory Team did not have the permission to distribute the FRMAC products.

HHS

On May 12, 2003, HHS Headquarters in Washington, D.C., developed a plume prediction using DTRA's Hazardous Predicting Assessment Capabilities model. They used an unknown scenario to generate their inputs for the model. Observations by data collectors suggest that they developed the plume projections to identify HHS assets that might be required and eventually deployed. These maps were used to brief the HHS Secretary and DHS Secretary during the FSE. Since the model used to generate the HHS plume prediction differed from the one used to generate the DOE plume prediction, it is likely that the outputs differed as well.⁷⁷

NOAA

NOAA also generated plume predictions during the exercise. They too used unknown scenario estimates to input into their model. In addition, NOAA used real weather patterns for their model rather than the canned weather planned and used during the T2 FSE. NOAA intended to run their model for training purposes only, and the resulting plume prediction was to be walled off from inter-agency play. Nonetheless, copies of the maps were faxed to the DOE Headquarters during the exercise. The addition of another plume prediction generated with yet another model and resulting in a different output from the two others may have added to Federal top officials' frustrations.⁷⁸

EPA

The evaluation team does not have any data to indicate that the EPA Headquarters generated a plume prediction during the exercise. However, there are data that indicate that the White House contacted EPA Headquarters for a plume map.

4. Artificialities

A number of exercise artificialities contributed to the data coordination and analysis product distribution challenges were observed during T2. These included:

- The JOC was closed from 2300 on May 12, 2003, until 0700 on May 13, 2003;
- There was an insufficient number of controllers to provide injects to agency personnel collecting radiological data at the RDD incident site. This was especially problematic during the overnight hours of May 12 to May 13, 2003. In addition, the WA DOH RMAC did not have an exercise controller located in their facility;
- The FRMAC expected the affected area to become smaller over time due to the re-wetting of contaminated material. However, exercise controllers did not have the pre-scripted data to support the re-wetting process;
- The location of the FRMAC was unrealistic, as it was located in a contaminated area;
- While there will always be security at an incident site, particularly if WMD are suspected, security during the FSE was slow and cumbersome; and

⁷⁷ The evaluation team does not have sufficient data or plume prediction maps to compare the results from the different models

⁷⁸ Again, the evaluation team does not have sufficient data to compare the results from the different models.

- The events leading up to the RDD at the Columbia Generating Station would have caused most State assets to be deployed to Richland. This would have delayed their response to the RDD incident in Seattle by hours.

5. Analysis

a. Plume modeling

As described in the reconstruction, the Seattle EOC contacted NARAC soon after the explosion to have them generate a prediction for where the plume would travel. The resulting product was made available to the King County and WA State EOCs as well as the FEMA ROC and other Federal and State agencies. To add to the confusion, the State DOH RMAC generated another plume prediction using the HotSpot modeling program, once they obtained enough data to input a reliable source term.⁷⁹ As described in the reconstruction, the RMAC used EPA's wireless Internet capability to send their plume prediction to the WA State EOC. As a result, Seattle, King County, and Washington State top officials all had different information from which they could make their preliminary decisions. The evaluation team does not have sufficient data to determine whether each jurisdiction had multiple plume prediction maps or whether they simply had different plume prediction maps. In recognition of the fact that data availability is likely to be very limited early in an RDD response, WA State DOH, PHSKC, and EPA developed default PAGs, based on the existing PAGs, to use during an RDD event. The Seattle Mayor applied these "default" PAGs during the early hours of the incident, as decision-makers awaited the collection of the data required to effectively model the release. Therefore, it is not clear if the presence of different plume predictions affected local and State top official decisions in the early hours of the exercise.

In addition to the confusion in Seattle, several Federal agency and department headquarters developed their own plume predictions to make internal assessments concerning assets that might be required. These Federal agencies and departments all used an unknown scenario to generate input data and used different models to generate plume predictions. So even if the input data were the same, the output may well have differed. As noted earlier, the evaluation team was told that many of these agencies generated the predictive maps for internal purposes—either for training purposes or to provide them with some insight into what Federal assets might be needed for the response. Nonetheless, during the T2 FSE, multiple maps from the predictive models were presented to department and agency top officials in Cabinet-level meetings. This led to some confusion and frustration by top officials in Washington, D.C., as to which output was the correct one to use. Although the evaluation team did not identify that the existence of multiple maps produced any direct consequences upon decisions made during the FSE at the Federal interagency level or in Washington State, the issue may have contributed to delays in decision-making. This underscores the role of the FRMAC as the single place to coordinate and analyze data, and to provide authoritative data products to support decision-makers, in accordance with the FRERP. Decision-makers need to understand that this process takes time, and that the empirically-based data products provide more accurate information than initial plume predictions. Furthermore, it is easy to imagine the possible consequences of FSL governments producing many different maps, particularly if they have used different measurements and standards.

⁷⁹ The evaluation team does not have sufficient data or plume maps to compare the results from the different models.

While it didn't happen during the FSE, the media could have questioned the FSL governments' expertise and ability to make decisions.

In the region close to the incident site where protective action decisions are most important, estimates based on atmospheric models are very uncertain. For very large-scale decision-making (e.g., identifying the ingestion pathway), models may be more useful but are generally applied with conservative assumptions that reduce their usefulness. In the case of TOPOFF 2, projections exceeding FDA criteria out to 150 miles from an RDD in downtown Seattle were not credible and potentially could have resulted in unnecessary food protection actions.

Finally, and possibly most importantly, it appears that few decision-makers were informed of the fact that a plume prediction has a limited useful lifetime. As discussed in the introduction to this section, model predictions need to be continuously updated using real measurement data, and will be replaced by products generated primarily from measured data, once enough data are collected, interpreted in a manner understandable to top officials, and the resulting products distributed. During the FSE, top officials emphasized their frustration regarding the different plume maps. However, they did not ask for (or in some cases receive) updated information that relied on empirical data. This suggests there is a need for additional education among both responders and decision-makers regarding the timing and value of the different types of information following an RDD explosion.

b. Data collection and coordination

As described in the reconstruction, there was minimal coordination of radiological data collection between FSL agencies at the incident site or at off-site locations until the third day of the exercise. Many FSL agencies with various data collection capabilities arrived to the incident site at different times. As in any mass casualty incident, Incident Command has many responsibilities, including the primary mission of rescuing victims, all of which require the Incident Commander's attention. This can easily stress incident command capabilities, and limit attention to many tasks—particularly relatively specialized or complicated tasks.

During the FSE, there is evidence to support the fact that the Incident Commander tasked the EPA field team and the CST to work together to coordinate monitoring and sampling at the site, and report their data to the HAZMAT Chief. While there is evidence that WA DOH RMAC was in contact with Incident Command, it is unclear what information was shared. However, there is no evidence to indicate that WA State DOH RMAC coordinated their collection efforts with the Incident Commander or with the HAZMAT Chief. Rather, the data indicate that the Washington DOH RMAC, DOH field teams, and the Washington State Department of Ecology field team coordinated with each other on May 12, 2003, but not with the other local or Federal data collection agencies at the incident site. By May 13, 2003, the EPA and DOE RAP teams were also coordinating with the DOH RMAC.

The result of the on-site coordination failure is that no one agency at the incident site had all of the data. In addition, some responders entered contaminated areas to collect data that another agency had already collected, which meant they were exposed to more radiation than necessary. As a consequence, FSL responders, collecting data for different purposes, duplicated on-scene efforts. As an example, during the on-scene Hotwash, EPA learned that a bomb squad had sent robots into the most contaminated areas armed with radiation meters, which were then read from a distance using cameras. Because this data was not integrated in the incident command system

and shared with all responders, EPA field teams later collected these same data points again, resulting in perhaps unnecessary exposure of personnel to radiation. In addition, as the uncoordinated data left the incident site, different jurisdictions (i.e., Seattle, King County, and Washington State) had different data from which they developed information to make recommendations and decisions.

While coordination challenges on the ground and among agencies are to some extent expected early during the incident response, the arrival of the FRMAC (2000 on May 12, 2003) is designed to facilitate at least more organized off-site data coordination. As discussed in the *Background* of this section, one of the first steps the FRMAC typically takes upon arrival at a radiological incident is to hold an advance party meeting with representatives from the State and other Federal agencies. The advance party meeting is designed to facilitate relationships with relevant Federal, State, and local officials, and to put processes in place to facilitate the coordination of data and the distribution of information to all relevant agencies.

During the FSE, the advance party meeting did not occur. DOH staff at the WA State EOC made the decision to not send a liaison to the FRMAC based on how busy DOH personnel were in the opening hours of the FSE and a lack of understanding of the importance of the advance party meeting and co-location with the FRMAC. To further complicate issues, that decision was not communicated to the RMAC; so they were unaware that the FRMAC had even arrived. The lack of an advance party meeting meant that neither State nor Federal agencies had the opportunity to develop and agree on procedures to send data to a single analysis location—which presumably would be the FRMAC. As a result, the only data the FRMAC had on May 12, 2003 was from the AMS and from their field monitoring teams. As described in the reconstruction, the FRMAC did not receive data from the RMAC, EPA, or the DOE RAP Teams until May 14, 2003. The lack of on-site coordination also makes it unclear if the FRMAC ever received data collected by the SFD HAZMAT Team.

EPA participants suggested a possible means of supporting coordinated data collection efforts. They suggested that it would have been beneficial if all of the technical agencies collecting data at the incident site had come together to present unified recommendations on roles and responsibilities to the Incident Commander. They also suggested that it would have been beneficial for one of the technical agencies to volunteer to coordinate all of the data being collected on the site. Although this might have helped coordinate the data, it would require one of these support agencies to take the lead in coordinating the effort. A potential middle ground would be for Incident Command to track which teams are on-site collecting data, and task one of the support agencies to coordinate the effort. This would provide Incident Command with both the unified front they lacked during the T2 FSE, and an SME to coordinate and possibly provide expert advice. Further, this would give these critical SMEs greater visibility with Incident Command than they had during the T2 FSE, where they were working for the HAZMAT Chief—two levels below the Incident Commander.

Data collection, management, and distribution continue to be a challenge at nationally significant incidents. FRMAC procedures, which were developed primarily for radiological releases from a fixed nuclear facility, should be re-examined to ensure that they are effective in handling non-fixed facility incidents involving on-scene response by FSL responders. Although the plan was modified since its original inception, the procedures remain modeled on response methods appropriate for nuclear reactor disasters. Further, the Washington State DOH Procedures for Responding to a Radiological Attack is written to integrate into existing FRMAC and other DOE

plans. When applied to terrorist events, like that simulated during T2, there are differences that may impact the effectiveness of these procedures. These include:

- Disasters at nuclear facilities are likely to involve known radiological materials and estimates of quantities involved, whereas the materials and quantities used in terrorist-sponsored RDD explosions are not known until analyses can be completed, as was the case in the T2 FSE; and
- Terrorist activities are more likely to occur in major metropolitan areas with high profile, politically powerful, and well-equipped local governments; whereas nuclear facilities tend to be in rural communities with fewer response assets. In Washington, the DOH Procedures for Responding to a Radiological Attack only acknowledges a local jurisdiction's leadership role at an incident when "command shifts or transitions to local jurisdiction," rather than assuming that the local jurisdiction is in charge and that the State is a support agency⁸⁰. This may stem from their experience or responsibilities for nuclear power facilities, or their internal expectations.

As DHS develops its plans for responding to radiological (and other) emergencies, it is imperative that they build in processes that allow State and local government capabilities to be coordinated with the federal capabilities. This is particularly important because state and local resources are likely to arrive on the scene and begin using their assets before the federal support arrives.

Another issue that deserves further attention is whether the FRMAC should release raw data sets to different agencies, or to continue to send out only data products. In T2, the FRMAC policy was to collect and analyze data locally, and only send out data products. A number of Federal and State agencies suggested that they need the raw data to conduct their own analyses, and that the FRMAC policies do not allow them to meet their missions. However, were data to leave the FRMAC, there is greater potential for many agencies to have incomplete or out of date data. This could further complicate the coordination challenge and increase the likelihood of inconsistent decisions and public information.

c. Data analysis, distribution, and impact on decision-making

Developing the most valid deposition maps possible requires that all data be sent to the SMEs who are interpreting the data. As far as the evaluation team has discerned, the radiological data collected by the SFD HAZMAT never left the incident site, and might not have been used to develop deposition maps. In addition, there is no evidence that any of HAZMAT data were sent to the RMAC or the FRMAC to support their analyses. Therefore, it is quite likely that none of the agencies analyzing radiation data were using all available data. This is one reason that different analyses could result in different information being sent to top officials. As described earlier, the WA DOH, Public Health Seattle/King County, and EPA recognized the likelihood of limited data reaching decision-makers early in an RDD response and developed default PAGs prior to the FSE. The Seattle Mayor used these default PAGs during the early hours of the incident.

⁸⁰ Washington State Department of Health, *Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack*, DOH/DRP, March 2003.

However, even if the data coordination challenges did not exist, analysis product distribution was another challenge for responders during the FSE. Prior to the arrival of the FRMAC, the WA State DOH, King County EOC, and PHSKC plotted rough deposition maps using data collected by the WA DOH field teams.⁸¹ As noted in the *Reconstruction* section of the AAR, lack of resources made it difficult, if not impossible, for these maps to be interpreted and reach decision-makers in a timely fashion. Therefore, significant data points served as key discussion points during conference calls to help top officials make decisions.

The impact of the lack of clear information led to significant frustration among top officials. A number of T2 data collectors observed the frustration and noted players' attempts to resolve the frustrations on their own. For example, at 2100 on May 12, 2003 a data collector at the Seattle EOC recorded that the Mayor's representative told the WA DOH that they wanted to make-up their own data to develop the information they needed to define an evacuation route. A data collector recorded similar statements at the WA State EOC. Although the evaluation team does not know whether Seattle or Washington State followed up on its quest to make up radiological data, these observations do illustrate the problem.

The evaluation team identified four potential contributing factors that may have led to the frustration experienced by the State and local top officials during the overnight hours of the exercise:

- It is likely that there was insufficient scenario data during the overnight hours (see *artificialities*);
- Controllers in the WA State EOC gave conflicting information to DOH personnel and also withdrew information that had been provided earlier in the exercise;
- As described in the reconstruction and in the previous section, there was also a lack of effective coordination, until the third day of the exercise; and
- It is possible that top officials did not recognize the real amount of time that it takes to collect, coordinate, and analyze data and present it in a meaningful fashion. Many top officials are used to participating in tabletop exercises where the data and information they request are made available much more quickly than would happen in real emergency—in tabletops, data and information are often available instantly.

The timing of the statements showing top official concerns on May 12, 2003, suggest that some of this frustration might have been alleviated if the EOCs had received the FRMAC analysis products sometime during the first night of the FSE. In a conference call at 2000, the PFO assured the State and local officials that the DOE would provide them with AMS data once they were received and analyzed. However, as described in the reconstruction, it took longer than the PFO expected for the FRMAC to complete the analysis of the AMS data; the analysis products were not completed until after the JOC closed for the night. This exercise artificiality may have led to, or possibly exacerbated, frustrations because local and State officials then had to wait a minimum of eight hours to receive the information they needed.

Although the JOC re-opened at 0700 on May 13, 2003, the FRMAC did not deliver their deposition map to the Seattle or WA State EOCs until mid-day on May 13. As a result of not

⁸¹ The evaluation team does not know whether Seattle EOC or incident command were plotting data in a similar manner, or whether the various EOCs shared their deposition maps.

having the advance party meeting on May 12, 2003, the FRMAC did not have the appropriate contacts within the various EOCs. If the FRMAC had the contact information and the clearance to provide maps directly to Seattle, King County, and WA State EOCs, the FRMAC might have supplied them with the deposition data product map as early as 2330 on May 12, 2003. It is highly likely that had the JOC remained open throughout the night, the FRMAC would have received clearance to distribute the deposition maps and would have identified the appropriate contacts at the Seattle, King County, and State EOCs, as each jurisdiction provided liaisons to the JOC.

It appears that after the FRMAC deposition maps were distributed to State and local EOCs, there was less confusion over which information to use for decision-making. The distribution process was flowing well by the end of play on May 13, 2003, and continued rather effectively on May 14, 2003—at least in Washington State. Regionally, the players' were well aware of the problems, and found ways to resolve them. However, the concerns in Washington, D.C., did not seem to end, even after the exercise was over. Nonetheless, there is no evidence that activities at the Federal inter-agency level or the different data products provided to these top officials had any impact on the response in Washington State.

6. Conclusions

Several lessons can be learned from the data coordination and analysis product distribution challenges faced by responders and top officials in Washington State and Washington, D.C. Plume models provide a prediction of where the material in the explosion will travel. They can be useful in assisting decision-makers in making preliminary decision regarding likely areas of contamination. Once actual data from the incident are collected and evaluated, the value of plume models diminishes. Once responders learn what really is out there and where it is, predictions alone become less important. However, predictions updated with initial measurement data can be useful in estimating protective actions in areas that have not yet been surveyed, or in areas that have been contaminated below the measurement threshold of available instruments. During the FSE, WA State DOH and Federal SMEs could have provided top officials with this information. Additional educational opportunities might have been available in many months leading

SUMMARY OF CONCLUSIONS— DATA COLLECTION AND COORDINATION:

On-site and off-site data coordination during the FSE was minimal at best. As a result, no one agency at the incident site had a complete operational picture, and multiple agencies were performing redundant tasks. The development of National Incident Management System may help to facilitate the data collection and coordination processes in the future.

There was much confusion during the FSE about the multitude of plume prediction maps among agencies and across jurisdictions. While it did not happen during the FSE, if agencies and jurisdictions produce inconsistent and conflicting maps, the media could question the governments' credibility and ability to make decisions.

Officials at all levels of government need to be educated about the differences between plume dispersion prediction models and data products generated from empirical data. Officials need to be aware of how each can aid decision-makers and the limitations of both.

FSL agencies and departments should be educated about the need to coordinate the data collection and distribution processes and the implications of a lack of coordination.

Plans and procedures for radiological incidents were initially developed for emergencies at nuclear power facilities. To be effectively applied to terrorist events, these plans and procedures may need to be modified.

On-site data collection may also benefit from the designation by the Incident Commander of a support agency to lead the coordination effort.

up to the FSE.

On-site and off-site data coordination was minimal at best. For SMEs to develop the most up-to-date information and provide the highest quality recommendations, it is critical that they receive data collected from all relevant locations. During the T2 FSE, the coordination to send all of the data to one place was lacking. One aspect of the response that became clear during the FSE was that there are many assets with radiological data collection capabilities at FSL levels of government that need to be accounted for in the data collection process. In planning responses to terrorist attacks, procedures need to recognize all of the possible responders, and work to ensure that they are coordinating effectively. The development of the National Incident Management System (NIMS) may help to facilitate the data collection and coordination processes in the future.

In addition to the FRMAC, many State and local government agencies have their own capabilities and responsibilities to generate plume predictions and deposition maps. In an emergency, State and local governments are likely to rely on their assets before Federal assistance arrives, and to continue to rely on them throughout the response and recovery. The Federal Government cannot prevent other FSL agencies from using their own models and developing their own predictions for internal planning purposes. However, FSL agencies and departments can be educated about the importance of centralizing the data collection and analysis product distribution processes and learning to work with the FRMAC to coordinate efforts during radiological emergencies and the consequences if that does not happen.

E. Play Involving the Strategic National Stockpile

1. Introduction

In Illinois, during the Top Officials (TOPOFF) 2 (T2), the arrival, breakdown, distribution, and dispensing of the Strategic National Stockpile (SNS) was played in unprecedented detail during the Full-Scale Exercise (FSE). It culminated in the dispensing of thousands of doses of simulated medication to role players at five separate sites, in five jurisdictions. However, perhaps of even greater interest than the actual distribution were the discussions and decisions leading up to the distribution activities. Officials had to determine:



- How to request the SNS;
- Who should receive the medications;
- How much was available;
- When and where to distribute it; and
- How to announce it to the public.

This account focuses on how the local municipalities dealt with the issues of providing prophylaxis to both first responders and the public. It also examines decisions made about the SNS at the inter-agency level.

2. Background

Created in 1999, the SNS is a national repository of medications and other supplies and equipment that can be deployed in the event of a terrorist attack. Formerly known as the National Pharmaceutical Stockpile, the SNS was renamed upon its transfer to the Department of Homeland Security (DHS) in 2003. The SNS is a multi-agency resource, with responsibilities split across DHS, the Department of Health and Human Services (HHS), and the Veterans Administration. According to a recent Memorandum of Agreement among the three departments:

The DHS Secretary shall, in coordination with the HHS Secretary and the Secretary of Veterans Affairs, maintain the Strategic National Stockpile.

The DHS Secretary shall be responsible for the overall strategic direction, goals, objectives, and performance measures for the Stockpile.

The DHS Secretary shall be the owner of the Stockpile and the assets (excluding personnel) of such Stockpile shall transfer to the DHS Secretary. The Stockpile shall remain in the physical custody of the HHS Secretary until deployed by the DHS Secretary.

The DHS Secretary, in consultation with the HHS Secretary, shall direct the deployment of the Stockpile, determine pre-position locations and shall have the responsibility for authorizing the transfer of custody of Stockpile contents to State or local authorities.

However, while giving ownership of the stockpile to DHS, the Memorandum of Agreement assigns management responsibilities to HHS:

*In consultation with the DHS Secretary, the HHS Secretary in managing the Stockpile shall determine for the Stockpile the appropriate and practical numbers, types, and amounts of drugs, vaccines, and other biological products to provide for the emergency health security of the United States.*⁸²

The Centers for Disease Control and Prevention (CDC) maintains the SNS within HHS.

The SNS consists of two parts: the 12-hour push package (push pack) and Vendor Managed Inventory (VMI). CDC maintains 12 push packs strategically distributed at ten sites around the nation. Upon release by the CDC, the SNS can deliver a push package to the site of an emergency in 12 hours or less. Thus, it can be deployed before the specific infectious agent has been confirmed. Each push pack contains more than 50 tons of supplies. Depending upon the infectious agent, a push pack can treat from several thousand to several hundred thousand people. In a large bioterrorism incident, the VMI can also be deployed. It's tailored to contain the specific medications to treat victims of a known agent. The VMI can arrive in the affected area within 24 to 36 hours. Either the VMI or the push-package can be shipped first, depending on the situation.

Illinois also maintains its own pharmaceutical stockpile, known as the Illinois Pharmaceutical Stockpile (IPS), and some localities maintain their own stockpiles of medications. The IPS is designed for use by immediate responders.⁸³ Use of these stockpiles was also played during the FSE.

3. Reconstruction

a. Overview

The SNS Operations Center (SNSOC) was activated at 1500 EDT May 12, 2003, based upon a directive from DHS. In a conference call at 2000 EDT, HHS Secretary's Command Center (SCC) directed that two SNS sites nearest to Chicago be readied for loading onto planes. It is not clear, however, whether the SNSOC received this directive. The SNSOC did receive a directive from DHS to pre-deploy a push package to the Chicago area, which it did. The City of Chicago, followed closely by the State of Illinois, requested the SNS early on the afternoon of May 13, 2003, immediately after a bioterrorism incident involving the release of Pneumonic Plague was confirmed. The next morning, officials publicly confirmed that there had been a release of plague at the United Center, O'Hare International Airport, and Union Station, and only at these three sites. At 1025 Central Daylight Time,⁸⁴ the push pack arrived at O'Hare. It was distributed to the local jurisdictions that afternoon, after which most jurisdictions issued prophylaxis to their first responders. The follow-on VMI supplies began to arrive at 1937 on May 14, 2003. The distribution sites were opened to the target population at 0800 on May 15, 2003, at the same time that the Virtual News Network (VNN) announced the distribution

⁸² Memorandum of Agreement between the Department of Health and Human Services and the Department of Homeland Security concerning cooperative arrangements to prevent, prepare for, and respond to terrorism and major disasters, signed February 28, 2003 and March 5, 2003.

⁸³ Illinois Department of Professional Regulation State Board of Pharmacy, [Newsletter] Feb 2003.

⁸⁴ All times provided are Central Daylight Time, unless otherwise noted.

locations and listed the target population. Figure 15 depicts the timeline of events related to the request for and distribution of the SNS.

Strategic National Stockpile

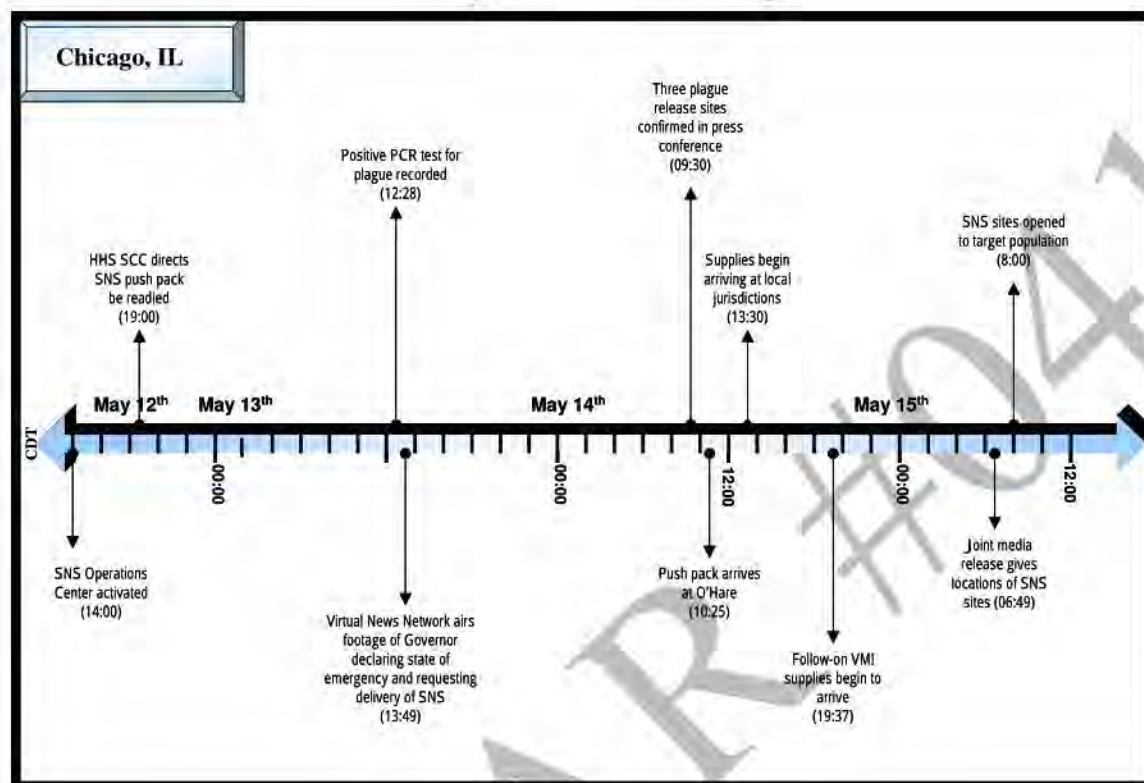


Figure 15. Timeline of Events Related to the SNS

b. Initial discussions

Decisions and activities relating to the SNS took place at all levels of government. On the morning of May 13, 2003, before diagnosis of plague, discussions began at local and State departments of public health (DPHs) about the need to provide prophylaxis and to request and activate pharmaceutical stockpiles—local, state, and national. The SNS also came up in discussions at the Federal Emergency Management Agency (FEMA) Region V Regional Operations Center (ROC); the HHS Region V Regional Emergency Operations Center (REOC); the County, City, and State Emergency Operations Centers (EOC); HHS Headquarters; DHS Headquarters; and the Strategic Information Operations Center (SIOC) in Washington, D.C.; and the CDC in Atlanta.

HHS had already alerted CDC to have the SNS ready to go. On May 12, 2003 at 1900, anticipating a rise in the threat condition to Red, HHS directed CDC to put the stockpile on planes, with the two closest to Chicago ready to go. At 1946, having heard that threat condition was raised to Red in seven cities, the HHS Assistant Secretary Public Health Emergency Preparedness told his staff to notify CDC to load the planes—a standard operating procedure for the CDC upon Red being declared.

At 0800 on May 13, 2003, CDC reported that the SNS was being deployed to Chicago. At 1030, the CDC Director reiterated public health priorities. One of these was to focus on the immediate needs of Chicago, as well as Seattle which had just experienced the detonation of a radiological dispersal device (RDD), but not to over-commit CDC resources, as there was a potential for multiple terrorism events in other parts of the country. In an 1100 conference call with HHS, the ROC, and the REOC, CDC reported that the SNS could be delivered to Chicago within an hour. At 1228 the Chicago, Illinois Department of Public Health (IDPH) lab recorded a positive Polymerase Chain Reaction (PCR) test for plague. However, it wasn't until 1415 that CDC received notification of the positive PCR; at that same time the confirmation of plague was announced on VNN.

On May 13, 2003, at 1730 EDT, HHS Secretary Thompson declared a public health emergency in the City of Chicago, allowing HHS to provide federal health assistance under its own authority.

c. Requesting the stockpiles

In Illinois during the afternoon of May 13, 2003, local jurisdictions and the state declared a state of emergency and requested the SNS. There was some confusion as to when declarations were officially declared by the individual jurisdictions. At 1253, the FEMA ROC log noted that the City of Chicago was requesting the SNS; a similar entry regarding an urgent request from the state was logged at the ROC at 1325. Discussions about requesting the SNS occurred at the DPHs starting about 1330. At the DHS Crisis Action Team (CAT) at 1430, there was discussion of deploying the SNS. A request from the City of Chicago for a push pack showed up in the Department of Homeland Security (DHS) Homeland Security Center (HSCenter) at 1528 and at the CDC around 1600.

At 1250, VNN aired footage of the Illinois Governor reporting that that he had declared a state of emergency in Illinois, requested a disaster declaration from the President, and requested delivery of the SNS. At 1410 the Illinois Operational Headquarters and Notification Office (IOHNO) reported that the Illinois State EOC would request the SNS (push pack and VMI) through the Governor's office; at the same time Cook County DPH checked with the state for procedures.

At 1515, IDPH notified the SEOC to ask for surgical masks and ventilators as part of the VMI request. Later that afternoon, in a conference call at 1655, discussion ensued about procedures for requesting the SNS. IDPH went directly to CDC, whereas the Illinois Emergency Management Agency (IEMA) went to the ROC. On May 14, 2003, at 0935, IOHNO logged specific requests from the VMI for Doxycycline, Ciprofloxacin, masks, and ventilators.

d. Who should receive antibiotics

Internal debates about a prophylaxis distribution policy for first responders, including non-governmental organizations such as the American Red Cross, and the public occurred in all local jurisdictions. These discussions were necessitated not only by the enormous logistical challenges of distributing medications to a metropolitan area whose population exceeds seven million, but also by the very real limits of the amount of medication that was immediately available.

In the end, all jurisdictions except Chicago decided to provide prophylaxis to all first responders. Chicago was unable to do this due to the sheer size of their first responder population, estimated

at 96,000, and because officials felt it would be politically untenable to provide medications to all of the first responders before the providing the same for the general public.

The distribution of simulated local pharmaceutical stockpiles was demonstrated in Chicago and DuPage County. Chicago DPH administered prophylaxis from its own stockpiles to Chicago DPH staff (on May 13, 2003, at 1640). DuPage County followed its protocols and administered its stockpile to its first responders and their immediate families (a decision made at 1326 on May 13, 2003) and County employees (distribution began at 0914 on May 14, 2003).

Within the Lake County EOC, there was a discussion as to how many people in each category should receive prophylaxis. They also discussed who would make the decision about how many people to provide prophylaxis for. In the end, they decided on all first responders per protocol.

Both Cook County and Lake County issued prophylaxis to first responders at 1600 on May 14, 2003; it is unclear whether they used the IPS or the SNS. Chicago, however, issued medications to a single shift of first responders only: those on duty during the early morning hours of May 15, 2003. They did not distribute the antibiotics earlier due to a miscommunication; they believed that all jurisdictions had agreed to delay distribution of the SNS to anyone until 0800 on May 15, 2003. Chicago learned that the other counties had already distributed to first responders via an email at 1926 on May 14, 2003, stating that all Cook County first responders had received prophylaxis. At that point they began to make plans to do their own, partial distribution to first responders. At 2039 on May 14, 2003, a broadcast fax advised the Chicago district watch commanders to pick up prophylaxis packages; they were distributed to police officers beginning at 0032 on May 15, 2003.

As far as prophylaxis for the general public, there was also a city/county divide. The counties initially decided to offer prophylaxis to their entire communities. Chicago, again, differed. In a conference call at 1300 on May 14, 2003, the counties and IDPH discussed the situation. That morning, the plague outbreak had been publicly linked to three locations: a terminal at O'Hare International Airport, the United Center, and Union Station. Ultimately, all realized that a common policy had to be adopted to prevent one jurisdiction from potentially being overrun by citizens of another that had decided upon limited distribution. That realization was helped along by a recommendation from IDPH, which called for a distribution targeted at the following:

- People who were in the United Center, O'Hare Terminal 3⁸⁵, or Union Station on May 10, 2003; and
- People who had household contact with any presumed or diagnosed cases.

Although some of the counties were unhappy with this policy and discussed overriding the decision, all eventually agreed to it.

Later that afternoon, at 1445, IOHNO noted that IDPH recommended and the counties concurred that an individual could pick up medications for other family members if he/she provided the required information.

Chicago's final decision, based upon a Chicago DPH recommendation, was announced at a 1730 EOC briefing: the first people to receive antibiotics were those in contact with cases, attendees at the venues, and first responders likely to be in contact with contaminated people (those on shift

⁸⁵ The release was later determined by consensus to have been Terminal 2, not Terminal 3.

when the drugs were distributed). They anticipated a quick backfill of antibiotics for the remaining first responders and their families.

e. How much was available

Confusion and contradictory information complicated officials' decision-making. First was the difficulty of determining the amounts in local stockpiles. Second were the issues about how much the state had and how the medication would be allocated. Finally, there were questions about how much would come from the SNS, when it would arrive, and how much each jurisdiction would receive.

An account of the confusion is documented here, focusing on the largest jurisdiction, the City of Chicago:

At 1715 on May 13, 2003, Chicago EOC requested 1.1 million doses of prophylactic antibiotics from IEMA, including 96,000 for first responders. Other jurisdictions requested lesser amounts; for example, Lake County requested 15,000 for its first responders and their families.

During a conference call starting at 1730, which included the FEMA ROC, IEMA, IDPH, and Chicago Office of Emergency Management (OEM), the OEM Director asked how many doses would be coming. IEMA replied, "enough, and will continue to re-supply." The city pressed for a number. IEMA said it was still determining the number. Chicago asked if this would be an open faucet, noting that its distribution schedule would depend upon the number of doses received. The ROC replied that the supply didn't seem to be a problem. Shortly thereafter, at 1818, the Chicago OEM director reported to his staff that the city was getting one million doses.

On May 14, 2003, IDPH decided that the stockpile would be broken out by jurisdictional populations. The IDPH Chicago office came up with these numbers for the initial distribution (a total of 45,800 doses⁸⁶) for the entire region:

- City of Chicago 12,400 doses
- Cook County 12,500 doses
- DuPage County 10,500 doses
- Lake County 6,000 doses
- Kane County 4,400 doses.

At 0917, the county health departments received a fax with these numbers.

About an hour later, however, Chicago DPH reported to the EOC that IEMA and IDPH said the city would receive 30,000 from the Illinois stockpile and 30,000 from the SNS. The Chicago DPH reported this again at 1150. They were expecting 60,000 doses available for Chicago.

At 1030, the Chicago OEM requested clarification during a conference call that included IEMA, the IL State EOC, and the Joint Operations Center (JOC). IEMA replied that the city would get 30,000 from the IPS and 12,400 from the SNS. However, at 1154 IDPH told Chicago DPH that the total of IPS and SNS doses was 30,000.

⁸⁶ It is not clear whether by "doses" they meant regimens (i.e. pre-packaged 10-day treatment courses). Each push pack contains pre-packaged regimens of Ciprofloxacin and Doxycycline.

The crisis over amounts of antibiotics available was definitively over at 1937 on May 14, 2003. At that time the IL State EOC announced in an exercise inject that VMI had arrived and that local health departments and hospitals would continue to be supplied for the length of the event.

The lack of clarity over available amounts illustrated by the above sequence of events can at least partially be traced to agencies sometimes co-mingling state and federal supplies, and also to a failure to separate out, in number and timing, the relatively small amounts in the push pack compared to the continuing flow of VMI.

f. When and where would the supplies be available

At 1730, on May 13, 2003, during a teleconference between FEMA, CDC, IEMA, and the governor's office, it was announced that the SNS would arrive at 1000 on May 14, 2003.

According to an exercise inject, the stockpile arrived at O'Hare airport at 1025 on May 14, 2003. It was transferred to a warehouse at 1055, at which time CDC signed it over to local authorities. The supplies were broken down and started arriving at the jurisdictions at 1330. Jurisdictions had pre-planned sites for distribution of the SNS to the target population, and an agreed-upon time for opening them. The distribution sites opened to the public at 0800 on May 15, 2003.⁸⁷

g. How were these decisions conveyed to the public

The public was informed that the SNS was available if needed by the Assistant Secretary Public Health Emergency Preparedness in HHS. At 1322, on May 13, 2003, the Secretary reported via VNN that the SNS was in the Chicago area and ready to be deployed. At 1527, VNN reported that the SNS was being rushed to Chicago.

A press release from the Office of the Governor early during the afternoon of May 13, 2003, indicated that antibiotics from the SNS would be distributed by local health departments to those with symptoms or those exposed. People with symptoms were told to go to the nearest hospital. Those exposed to the symptomatic were told to receive antibiotics.

In a press conference at the Joint Information Center (0930 on May 14, 2003), the three release sites, O'Hare International Airport, Union Station, and United Center, were confirmed.

On May 14, 2003, at 0940, IOHNO suggested on VNN that anyone who was at the three release sites should get prophylaxis. In a 1030 press release from the Governor's office, the Director of IDPH gave the same advice. At 1230 on May 14, 2003, the DHS Secretary on VNN advised all employees at the three sites to go to their doctors to get antibiotics. Chicago DPH, however, issued a press release stating "insisting that all Chicagoans stay at home until further notice, except for those adults considered to be essential to public safety....[and] those experiencing symptoms."

At 1259, on May 14, 2003, VNN announced that the SNS had arrived in Chicago.

At 1345, VNN announced that only 30,000 doses were coming to the Chicago area, whereas at 1745, a HHS official on VNN stated, "Once the faucet is turned on, the flow [of medication] doesn't stop."

At 1407, on May 14, 2003, there was a conference call that included the JOC, as well as the City and State EOCs about how to use the media to encourage people to stay home instead of rushing

⁸⁷ The Lake County site opened at 0832.

to the distribution centers. The message would be: “Stay home unless you’re in the exposed target groups; otherwise, going to the distribution site will increase your risk of infection.”

At 1425, in a conference call between IOHNO and CDC, consensus was achieved that a release would be issued that evening stating that distribution sites would be made public on the morning of May 15, 2003.

At 0800 on May 15, 2003, VNN issued details on distribution, identifying the locations and the target populations, including a change in who should go for medications. Symptomatic people were told to seek medical attention. Persons exposed to people with symptoms, those who had been at the three release sites, and those exposed to them were advised to go to their local distribution center.

At 0830 May 15, 2003, VNN reported that SNS had plague treatment for 115 million people.

4. Artificialities

None of the pharmaceutical stockpiles were actually deployed. SNS provided their training, education, and display package at the request of Illinois State to allow Illinois to test its ability to receive and distribute a push package. It is an exercise artificiality that the push packages were deployed at all. In a real event, the SNS reaction to requests for SNS would have been to send VMI, since pneumonic plague was already identified. It is unclear what the public reaction to the targeted distribution scheme would have been⁸⁸.

For reasons of space availability, the T2 scenario required that the SNS to arrive on the May 14, 2003, and be distributed at 0800 on May 15, 2003. This schedule gave decision-makers the luxury of time to discuss and determine in concert how to distribute the medications, and they didn’t even have to coordinate the time of distribution; it was given to them. In real life, pressures for a faster distribution would have made such coordination more difficult. With a compressed timeline and during a real emergency, jurisdictions might have made different, independent decisions and chaos could have been the result. In fact, discussions during this time period in the HHS SCC indicated continuing concern about the delays in opening the distribution centers.

Ultimately, the VMI was declared sufficient for the State’s needs. The health departments discussed offering mass prophylaxis after they were told that the amount of antibiotics was no longer an issue.

5. Analysis

The SNS story spans five of the areas of analysis and the inter-agency and Illinois venues. It is first and foremost the story of emergency public policy and decision-making regarding the allocation of a scarce resource. It involved jurisdictional issues at the Federal and local levels. It is also the story of local jurisdictions coming to separate decisions and then coordinating them (with some help from the state) to reach a common policy. Successful distribution required a coordinated, well-thought-out and accurate public information campaign.

⁸⁸ Dr. Henry W. Fischer, III, in his book, “Response to Disaster: Fact Versus Fiction and Its Perpetuation—The Sociology of Disaster,” predicts that panic would not ensue in a bioterrorism attack, but there is thankfully no data to draw upon to validate this prediction. Dr. Fischer does not specifically address the complications that could arise with the distribution of prophylaxis.

a. Decision-making

The key decisions regarding the SNS were who should get the antibiotics and in what order. To make those decisions, officials needed different types of information:

- Which antibiotics would be effective;
- How quickly would they need to be administered;
- How much was available;
- How long would it take to get the antibiotics; and
- How quickly could they be re-supplied?

During the FSE, decision-makers received conflicting information regarding the amount of antibiotics in the stockpile. Knowing the answers to the following questions would help officials better plan their strategy for distribution:

- Was there enough medication to provide prophylaxis to all first responders or would it need to be done in stages;
- If done in stages, would it be best (or possible) to provide prophylaxis to all those on duty and keep them on duty until sufficient supplies arrived for the rest;
- Or would it be better to give partial courses out to all first responders so that all could get started and then receive the rest of the course as more supplies became available; and
- How many sites should be set up for distribution to the citizens, considering the tradeoff between number of distributors (who also need prophylaxis) and number served?

Decisions made by the City of Chicago typify the importance of good information. Chicago, with its huge population, was the most hard-pressed jurisdiction.⁸⁹ It requested 1,063 million doses and waited for information from the state as to how much they would actually get. The state came back and said they could have 40,000 doses; however, it ended up with only 12,400. The city made distribution plans based on the 40,000 number. It chose not to provide prophylaxis to all first responders before reaching out to the public because it was concerned about adverse public reaction. Chicago decided instead to take a parallel approach, giving medications to current shifts of first responders, and at the same time providing medications for people who were at the three venues and the primary contacts of symptomatic patients. It is not clear if the city could actually have accommodated all of these people with the medications available to them at the time.

b. Resource allocation

The various pharmaceutical stockpiles constituted a scarce resource, at least until the VMI portion of the SNS began flowing. Some of the local jurisdictions had their own stockpiles, which they used to provide prophylaxis to different parts of their population: Chicago DPH gave antibiotics to its own staff; DuPage County administered its supply according to its phased plan,

⁸⁹ Cook County is almost equally large, but less data was available on their decision-making.

providing medication to first responders and their families and County staff and their families. The other jurisdictions apparently did not have their own stockpiles.

These differences raise policy issues. If some jurisdictions have their own stockpiles, should that be taken into account in allocating the supplies from other stockpiles? Such calculations appeared not to have been made, as the amounts provided to the localities from the state and local stockpiles were based upon population.

In addition, if the state issues guidance to medicate only first responders in advance of the general public, can a locality provide antibiotics to other segments as well out of its own stockpile? Would it then receive less from state and national stockpiles? Questions such as these become increasingly relevant as States and localities debate the advisability of establishing local stockpiles, given the difficulty of maintaining them.⁹⁰

c. Emergency public information

Public information play regarding the SNS had successes and failures. Some pronouncements were made that could have caused some measure of concern and confusion among the public. Several of these may have been due to erroneous VNN statements and not inappropriate judgments on the part of the officials releasing the information. However, a story such as the one describing the 30,000 doses that would be coming to Illinois (when originally there was believed to be 60,000 doses) could have caused chaos at medical facilities. And early recommendations from IOHNO, IDPH, and HHS that people at the release sites should obtain prophylaxis could have caused serious problems.⁹¹ These were made before the SNS had arrived and distribution sites had been set up. Tens, if not hundreds, of thousands of people who fit that description could have descended en masse upon medical facilities and pharmacies to get antibiotics that were not yet available. However, this problem is, at least in part, an exercise artificiality, as the consensus is that SNS play was artificially delayed.

In addition, conflicting advice was given about staying home and going out to get prophylaxis. Whereas IOHNO, IDPH, and HHS recommended that people at the venues obtain prophylaxis, Chicago DPH went on record “insisting that all Chicagoans stay at home until further notice, except for those adults considered to be essential to public safety....[and] those experiencing symptoms.”

The crafting of a joint press release about the SNS distribution at 0649 on May 15, 2003 was crucial to the success of the distribution and ultimately to containing the plague. Officials had to do their best to draw out those people who needed prophylaxis, while discouraging those who didn't from coming out and taking the limited supplies and/or unleashing unrest at the distribution sites. They agreed not to release the SNS distribution locations until the morning of May 15, 2003, to minimize the potential for civil unrest and chaos at the distribution sites. The release described who should seek prophylaxis (those at the release sites on the dates indicated, and those within six feet of someone displaying symptoms); where they should go; and when

⁹⁰ In June 2002, then IDPH Director John Lumpkin spoke against local stockpiles. When DuPage County asked about receiving reimbursement for the thousands of dollars it had spent on its stockpile, the Director of IDPH replied that, “Counties should not keep individual stockpiles because Illinois has an arrangement with a pharmaceutical company that keeps a current supply available that could be distributed to a county within a short period of time” [from the minutes of a DuPage County Board of Health meeting (6 June 2002)].

⁹¹ In the HHS statement, employees were singled out in the recommendation to receive antibiotics as they were presumed to have been exposed for a longer period.

they should arrive. It dissuaded those who hadn't been exposed from coming by reminding them that they would be safer at home, and stated that people with symptoms should go to the hospital, not the SNS sites.

However, this press release contained a flaw: it miss-stated one of the plague release sites. Confusion persisted throughout the FSE about which terminal was the release point at O'Hare International Airport. At various times, it was called Terminal 2, Terminal 3, and most frequently the International Terminal, which is Terminal 5. On May 14, 2003, around 1000, consensus was reached among public health departments that Terminal 2 was the correct terminal (which it was), but this information apparently was not passed on. When announcing who should get prophylaxis, the press release listed the international terminal as one of the three release sites. This may have been in part an exercise artificiality, as the myriad of reporters who would have covered this incident in real life would presumably have identified the discrepancies in public statements. But had they not, thousands of potentially exposed individuals could have been without drugs.

In addition, press releases about the SNS on May 14 and 15, 2003, contained conflicting information on the target population. There were several sets of somewhat differing guidance. The first concerned the dates of exposure. There were three variations:

- People who were at the sites on May 10, 2003;
- People who were at the three sites from May 10 to May 13, 2003; and
- People who were at the United Center from May 10 to May 14, 2003.

The second set concerned the description of who would receive prophylaxis. This set contained both internal inconsistencies and differences among jurisdictions. There were two variations. A press release from the DuPage County Board at 1811 on May 14, 2003, listed those exposed at the sites or those exposed to people with symptoms, and their entire families; however, this release also stated: "only people who have had direct close contact with infected patients should obtain antibiotics." A Chicago DPH press release at 0651 on May 15, 2003, listed those who were exposed at the sites and their close contacts, but only those household members who had been exposed to a person with symptoms. It's unclear whether these statements were actually released and whether the differences in them represented differences in distribution policy or not.

d. Coordination and communications

As noted earlier, miscommunication among the local jurisdictions caused the Chicago OEM to delay prophylaxis to its first responders while the counties went ahead with theirs. Had this played out in real life, it might have caused serious problems with the Chicago first responder communities. The Chicago OEM believed it had been told during a teleconference that none of the jurisdictions were distributing any prophylaxis until 0800 on May 15, 2003. This had financial repercussions as they had planned to dispense to first responders that evening; consequently, Chicago had police officers earning roughly one million dollars in overtime pay and doing nothing. When the OEM found out via routine e-mail that other jurisdictions had completed their first responder prophylaxis in the late afternoon of May 14, 2003, it put into play a partial distribution to first responders later that evening.

This misunderstanding can be traced to the medium of the conference call. Without written documentation of decisions reached, the potential exists for miscommunication. This was

observed throughout the FSE. During many teleconferences, roll calls were not taken, and it was unclear as to who was on the teleconference. In addition, on several instances different people heard different things and reached different conclusions about the outcome of the calls.

The conference call was useful as a means of coordination among agencies located far from one another and scattered among the EOCs. However, it was far from ideal as a reliable means of communication. These issues in the public health community were observed in TOPOFF 2000 as well, and were cited by the General Accounting Office in its September 2000 Report to Congressional Requestors titled, "West Nile Virus Outbreak: Lessons for Public Health Preparedness," and in which many officials reported problems in this area as the investigation into the outbreak grew. These problems could be ameliorated through strict adherence to roll call procedures and by designating one party to document any decisions reached and distribute them rapidly back to the participants via e-mail for confirmation.

e. Jurisdiction

The procedures and processes for requesting and receiving the SNS were a source of confusion throughout the exercise. Different jurisdictions took different routes to request this resource, and different agencies in the State also pursued their own paths. IDPH went directly to CDC, whereas IEMA went through the FEMA ROC; both of these are acceptable channels to request the SNS.^{92,93} It is unclear precisely what initiated the flow of prophylaxis. The two directives, one from DHS and another from HHS, regarding the deployment of the SNS provide one example of a jurisdictional challenge raised after the creation of DHS.

As noted in the background section, responsibility for this resource is shared between DHS and HHS. According to the Memorandum of Agreement, the decision to deploy the SNS is made by DHS in coordination with HHS. During the FSE, both HHS and DHS were giving directives regarding activation and deployment of the SNS. The SNSOC coordinated the stockpile deployment with the CDC and the FEMA EP&R Director. There is no data to indicate that senior-level consultation occurred between DHS and HHS. This issue was complicated when HHS declared a Public Health Emergency, which would allow it to deploy resources on its own authorities and at its own cost.

The following questions specific to the SNS were brought out during the course of T2:

- What is the process for requesting pharmaceuticals from State and Federal stockpiles;
- Does each jurisdiction have to submit its own request;
- Through whom do they issue the request;
- Can they request from multiple sources; and
- How much does one jurisdiction's request affect those of others?

The question of process arose despite the fact that there is a well-defined process for requesting the SNS (that should be a part of every public health agency's SNS distribution plan per CDC

⁹² It would be useful for DHS and HHS to clarify policies on how to request the SNS and educate the states on these procedures.

⁹³ Jurisdictional issues related to the SNS are discussed further in the *Core Area* on jurisdiction.

guidance). The official process involves a request from the governor or the mayor to the CDC, which then consults with DHS. There is no requirement for a disaster or emergency declaration.

6. Conclusions

The SNS was extensively exercised during the FSE. Local jurisdictions tested their ability to distribute supplies of antibiotics to their first responders and citizens. The state tested its ability to break down and secure the antibiotic stocks. Receipt, breakdown, distribution, and dispensing were completed successfully. But the SNS problem was far greater than the physical breakdown and dispensing of the push pack. It tested the ability of all levels of jurisdictions and agencies to make decisions, allocate resources, coordinate and communicate, and inform the public.

It is clear that work remains to be done in all of these areas. Pressures to make decisions under emergency conditions and tight timelines can be partially alleviated through thorough pre-planning and advance coordination amongst jurisdictions. The challenge is to figure out in advance the procedures for getting good information, sharing it widely, and making and documenting decisions in a coordinated way when operating under severe time pressure.

SUMMARY OF CONCLUSIONS— STRATEGIC NATIONAL STOCKPILE (SNS):

Overall, the receipt, breakdown, distribution, and dispensing of the SNS during the FSE were completed successfully.

The SNSOC coordinated the stockpile deployment with the CDC and the FEMA EP&R Director; there are no data to indicate that senior-level consultation occurred between DHS and HHS.

Miscommunication among local jurisdictions caused Chicago OEM to delay prophylaxis to its first responders while the counties went ahead with theirs.

Different agencies chose different avenues to request the SNS; this was a source of confusion throughout the FSE.

Conflicting and confusing information was given to the public regarding who should seek prophylaxis and when, the plague release sites, and whether one should stay home or seek medical attention.

This page intentionally left blank

F. Hospital Play in the Illinois Venue: Resources, Communications, and Information Sharing during a Public Health Emergency

1. Introduction

In the event that a highly contagious and lethal disease is spreading throughout a population, hospitals and other health care providers will become the first line of defense against a large-scale health catastrophe. How hospitals work with each other and the State and local public health authorities is critical to determining whether they will be successful in caring for patients and limiting the spread of the disease. Top Officials (TOPOFF) 2 (T2) presented an unprecedented opportunity to examine the coordinated efforts of the medical and public health communities to react to and control the spread of a disease outbreak. Because of the large number of participating hospitals, communication and resource requirements were significant.



During the T2 Full-Scale Exercise (FSE) an outbreak of Pneumonic Plague was simulated in the Illinois venue. Hospitals from the City of Chicago and the surrounding region participated in the exercise by receiving patients, and sharing information about resources. Hospitals coordinated, or needed to coordinate, in the areas of staffing and personnel, patient accession, the numbers and types of disease cases, diagnostic and treatment information, and diagnostic and treatment resources.

Hospitals used a range of technologies to share information about patients and resources. These technologies included fax, voice, Internet, phone hotlines, and call trees.

This special topic examines two critical issues surrounding hospital play during the FSE:

- How the hospitals communicated resource and patient information during the exercise; and
- What resources the hospitals had available to respond to the outbreak.

2. Background

In the Illinois venue⁹⁴ 64 hospitals⁹⁵ participated in T2. These hospitals exercised the Illinois Department of Public Health (IDPH) Emergency Medical Disaster plan by responding to both simulated paper and actual patients that arrived at their emergency rooms or were reported to infectious disease personnel. After seeing the patients, the hospitals reported syndromic and other information to the IDPH command center, and the Illinois Operations Headquarters and Notifications Office (IOHNO), located during the exercise in Springfield, Illinois. IOHNO in turn worked with the IDPH and the Illinois State Emergency Operations Center (EOC) (also located in Springfield) to develop an overall picture of the medical situation.

The IDPH disaster plan set up a hierarchical reporting structure for hospitals in the affected counties. Hospitals do not report directly to IOHNO during a disaster. Instead, hospitals within

⁹⁴ City of Chicago, DuPage County, Kane County, Lake County, and Cook County.

⁹⁵ The evaluation team has data from 60 of the 64 hospitals.

a designated region report to a “POD⁹⁶” hospital. The POD hospital consolidates information from the regional hospitals and then forwards it to IOHNO. Figure 16 illustrates this reporting process.

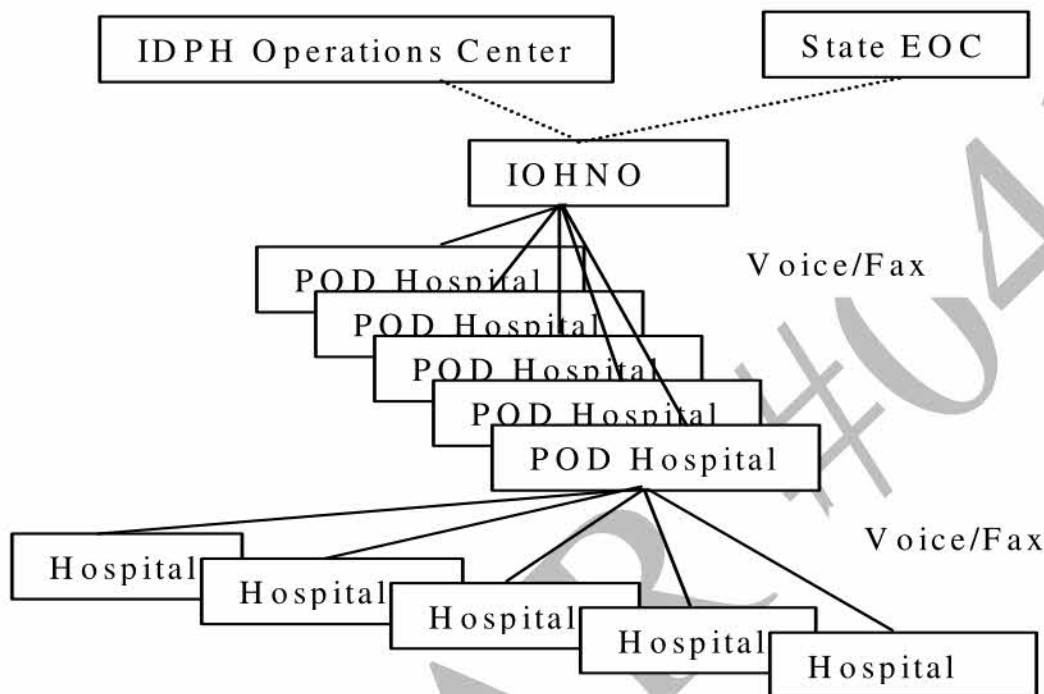


Figure 16. Reporting Architecture

The medical disaster plan was first activated at 0830 Central Daylight Time (CDT)⁹⁷ on May 13, 2003, in response to reported cases of Pneumonic Plague in DuPage County. The trigger was the result of an alarm on the DuPage County Pro-Net syndromic surveillance system. This system collected syndromic information from hospitals in DuPage County using a Web-based interface. The data collected are evaluated by software to determine if there are any unusual clusters or trends occurring. If an unusual spike in cases is detected the system alerts the local public health responders via a pager system. The initial alert on Pro-Net occurred at 1729 on May 12, 2003, due to an increase in respiratory patients at Edward Hospital, the first hospital to receive the simulated plague patients. In addition, the IDPH had sent a fax at 1545 to all hospitals on the subject of the TOPOFF Pulmonary Syndrome (TOPS). The fax was actually marked 2200 but was sent at the earlier time due to a controller miscue.

The detection of an unusual number of respiratory cases in DuPage County triggered Phase I of the Public Health Emergency Plan. Upon declaring a Phase I Emergency the POD hospitals are to contact hospitals within their regions and request information for the Phase I Disaster POD

⁹⁶ “POD” is not an acronym in this usage.

⁹⁷ All times referenced are CDT unless otherwise noted.

Worksheet. Table 6 lists the data elements collected on this worksheet. After collecting this information, the POD hospital is to transmit it to the IOHNO via telephone and fax.

Table 6. Data Elements from Phase I Worksheet

Emergency Department	Trauma Center	Adult Beds
Pediatric Beds	Total Other Beds	Total Units Blood
Ventilators Adult	Ventilators Pediatric	Ventilators Both
Field Bags	Decontamination Walking/hour	Decontamination litter/hour

The Emergency Medical Disaster plan data flow through the hospital emergency departments (EDs) then to IOHNO. During the FSE, patient data also reached IDPH through the infectious disease reporting system. By law hospitals have to report certain communicable diseases to their local health departments. This is usually done by the hospital's Infectious Disease Control Nurse who is to report incidents of diseases directly to the local (city/county) health departments. In turn the local health departments report to the IDPH Infectious Disease Control. During the FSE, the Infectious Disease Control personnel co-located with IOHNO in order to facilitate coordination.

Activation of Phase II of the Emergency Medical Disaster plan occurred at 1235 on May 13, 2003. Phase II activation was based on diagnosis of Pneumonic Plague in the suspicious respiratory cases. The Illinois Governor declared a statewide emergency at 1230 on May 13, 2003. In addition to the IDPH and state declarations, numerous city and county emergency declarations occurred during this time period.

Phase II activation requires additional, specific, information be reported by hospitals within the POD regions. Upon notification participating hospitals report information on the number of patients currently in the hospital, the type of conditions these patients have been admitted for, and the number of available beds of different types. The data are documented in Table 7.

Table 7. Phase II Resource Availability Worksheet. Hospitals Report the Number of In-patient Beds Currently Available for the Following Types of Hospital Care Beds

Medicine	Psych	Surgery	Orthopedics	Burns
Spinal Cord	OB/GYN	Pediatrics	Negative Air Pressure	Total

These bed totals are reported to the POD hospitals by telephone and fax, collected, and in turn reported by the POD hospitals to the IOHNO.

3. Reconstruction/Analysis⁹⁸

a. Communications and information flow

Throughout the exercise hospitals communicated with each other and the public health system to:

- Determine the status of beds, rooms, and supplies;
- Recall additional personnel as needed;
- Clarify the specifics of the exercise agent, including appropriate protection and treatment protocols; and
- Request assistance in the handling of the dead.

A variety of communication methods were employed during the exercise including phones, fax, in-hospital public address systems, pagers, radios, human runners, and amateur radio operators (HAM). These communications are summarized in Figure 17. The vast majority of all communications (eighty-six percent) were by either phone or fax. These transmissions included both those within each hospital and conversations/faxes to other hospitals and agencies within the emergency response community.

Hospital Communications

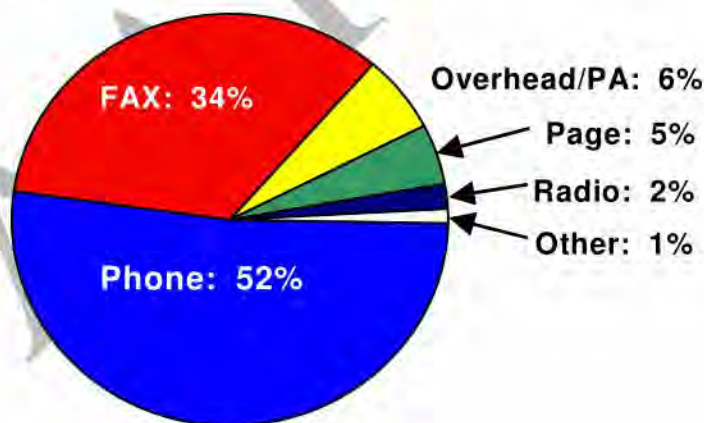


Figure 17. Hospital Communications (all transmissions, all targets)

Problems were noted with most of these communications routes. Telephone calls were hampered by problems with incorrect phone numbers, changes in contact phone numbers (at both

⁹⁸ This topic does not lend itself to a chronological reconstruction of events. The reconstruction is effectively an account and analysis of various dimensions of hospital response to the bioterrorism attack. For this reason, the Reconstruction and Analysis sections are combined.

the Illinois and Chicago Departments of Public Health) necessitated by extremely high in-bound call volume, and outbound call volume that caused difficulties in obtaining outside lines.

These problems caused delays in reporting resource information and also made it difficult for hospitals to recall staff through the use of phone trees. Call volume was the greatest problem; even exercise traffic exceeded some call switching capacities. For example, exercise traffic overwhelmed the phone system in south Kane County on May 14, 2003, necessitating the use of three HAM radio operators in order to maintain communications connectivity.

Faxes suffered from their own transmission and receipt problems due to call volumes. “Blast fax transmissions” from IOHNO, used to provide a wide variety of information and exercise updates, took up to two hours to complete. Some fax transmissions early in the exercise weren’t reviewed immediately because the receiving fax was in an office locked for the evening or not easily read by ED staff. Because of this, some hospitals designated individuals to staff the fax machine.

Radios were used primarily to communicate within a single hospital or between hospitals and incoming Emergency Medical Service (EMS) units. In addition, radios were used for backup communications at both St. Therese and LaGrange Hospitals during phone outages in the ED.

A great deal of effort was made during the exercise to obtain and update the listing of available resources reported by phone or fax. As shown in Figure 18, at least twenty percent of hospital exercise communications consisted of this type of reporting. It is important to realize that not only do these reports take time to send, but it also requires a great amount of time to obtain the information contained in these reports. The information consists primarily of bed counts, ventilator counts, and the number of rooms available at each hospital. Those counts were obtained either through additional phone calls to floors throughout the hospital or via walking the hospital floors to obtain the counts. This type of inventory effort was repeated throughout the exercise – usually at three- to four-hour intervals—at each of the 64 participating hospitals.

The remaining hospital communications consisted of notifications, mostly those associated with deaths. In addition, normal ED operations required a wide variety of contacts inside and outside of the hospital. A partial list of the individuals or departments called from the EDs includes: the hospital Chief Executive Officer and Vice President for Medical Affairs, the Command Center, floor nurses, the Intensive Care Unit, Infection Control, the Pharmacy and Blood Bank, housekeeping, and transportation.

Communications were also required among numerous agencies and organizations outside of the hospital, including, among others, the coroner, the American Red Cross, the Poison Center, the IDPH, and the county Department of Public Health (DPH), and the county’s Office of Emergency Management (OEM).

Bed, Resource Reports

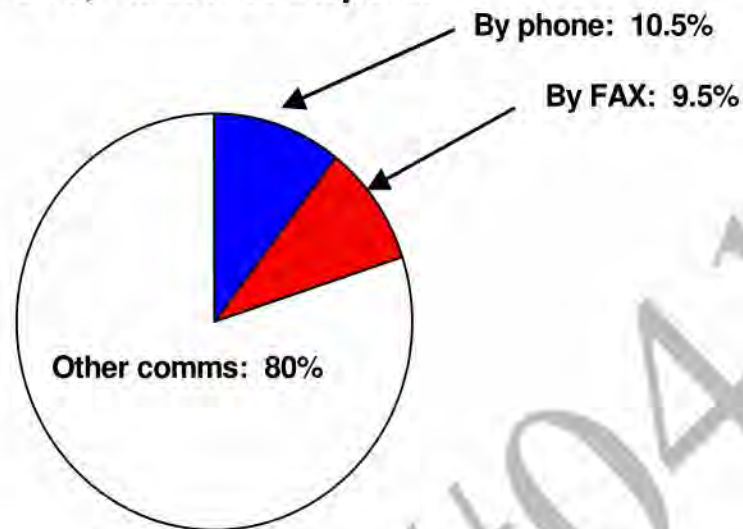


Figure 18: Hospital Resource Reporting

b. Beds

Twenty percent of all communications involved asking for and sending resource information. Counts of available patient beds were needed to determine if patient loads required additional resources, up to and including field hospital deployment. Therefore, as part of normal emergencies, individual hospitals provided bed counts to their coordinating POD hospitals, where the information was consolidated and sent to IOHNO.

During the exercise, a number of observations indicated that this process was difficult, at best. A data collector wrote, "An observation is this hospital is dealing with a large amount of paperwork—dealing with bed availability of POD hospital"

Some confusion existed as to the "why" of bed counts and the "which" of bed counts. For example, a data collector observed: "Discussion with physician about full disaster mode and purpose of meetings to know what beds available and sending patients as fast as possible to keep ER [emergency room] free."

The nursing supervisor talked to hospital staff about requesting a federal count, but there was confusion as to exactly which beds were to be included in the count.

At least six hospitals did experience maximum capacity situations, when either the entire hospital was full, or all the critical care beds or intensive care beds were in use. One hospital reached capacity at noon on May 13, 2003, two additional hospitals reached Intensive Care Unit (ICU) capacity shortly thereafter on the same day, and a fourth later that same evening. The next day's play filled the fifth hospital's ICU beds by noon. By early afternoon on Wednesday May 14, 2003, the sixth hospital's ED doctor indicated, "We're coming to the breaking point." At the same moment, the bed placement nurse commented to Hospital Admitting, "We are running out

of critical care beds.” Since Pneumonic Plague can cause severe respiratory disease, critical care and ICU beds will be at a premium if such a bioterrorism attack were ever to occur.

Types of beds needed to treat patients (as played during exercise)

During the exercise, a variety of bed types were specifically requested as part of normal medical treatment of the exercise patient population. These types included intensive care beds (ICU, Thoracic ICU, Mobile ICU, Pediatric ICU, and Surgical ICU beds), critical care beds in the Critical Care Unit (CCU), medical-surgical beds, other general medical floor beds, and pediatric beds. In addition to beds, monitoring capabilities were required for a portion of the patient population, and were requested as deemed medically necessary. The need for respiratory isolation and negative pressure rooms during the outbreak of a contagious respiratory disease was noted; the details of those specific requirements are discussed in the next section.

Bed use strategies and coordination

The FSE hospital play demonstrated the flexibility and creativity of hospital staff—as they juggled bed requirements for a significant influx of Pneumonic Plague patients. Different strategies were used to maximize the number of beds available to serve patient needs. For example, a wide variety of “other” beds were located throughout the hospitals and used for exercise patients. Throughout hospitals extra beds were found in Occupational Health, Ambulatory Care, Psychology, and Labor and Delivery. In at least five hospitals, additional beds were placed in the Endoscopy laboratory. The Physicians Treatment Center associated with another hospital was used for additional beds. One hospital also considered the suggestion that an entire wing be emptied, a suggestion that was not notionally implemented.

Significant numbers of personnel were directly involved in bed coordination efforts during the exercise. These included, but were not limited to, the following staff positions:

- Nursing Supervisor;
- Bed Coordinator;
- Bed Control;
- ED Charge Nurse;
- Nurse Manager;
- Case Manager;
- Doctors;
- Admitting;
- Maintenance;
- Registration; and
- Administration.

The coordination of this information was done through phone calls, fax, and hard copy tracking using dry erase boards throughout the exercise.

c. Staff

In addition to other resources, considerable staffing is required to respond to a major outbreak. The staff is required to treat and support the patient load, as well as support the administrative and command and control workload that will be placed on the hospital to support various coordination requirements. The FSE response proved to be no different. Staff phone trees were activated on both days of hospital play to recall doctors, nurses, and other staff to assist in the response efforts.

Staff recalls included not just doctors and nursing staff, but also receptionists and administrative personnel to handle paperwork requirements, housekeeping staff, technicians, computer personnel, and security, if lockdown procedures proved necessary. These individuals formed the basis for an emergency labor pool.

During the FSE, there were also other functions to which hospitals did not always assign a particular staff member. These jobs included persons to staff the radio full-time, staff the fax full-time, staff phone hotline(s) for the public, and assist in making phone calls.

Other infectious disease needs also require coordination to permit emergency personnel to work during an outbreak or a bioterrorism attack. These include childcare for the staff during the outbreak; one hospital's childcare facility notified the ED that they would stay late to accommodate staff needs. In addition, extended hours also mean that additional food and cots/beds are necessary during the outbreak.

d. Isolation rooms

Because of the recent Severe Acute Respiratory Syndrome (SARS) outbreak, the need for isolation and reverse pressure rooms has been highlighted, especially in the context of an unknown respiratory disease that may mimic SARS in its infectivity. These two types of requirements also played a role in the hospitals' responses to the T2 exercise epidemic.

Isolation Strategies

Three types of isolation levels were used in the participating hospitals. Initial patient presentations indicated the probable need for respiratory isolation and/or maintenance of the patient in a negative air pressure room. In addition, IDPH sent out an isolation directive on the evening of May 12, 2003. Later during the exercise, when the agent was identified as Pneumonic Plague, these isolation requirements were revised to the appropriate droplet protection level.

Because isolation rooms were in short supply, and at least two hospitals used up their supply of isolation rooms during the exercise, a number of alternatives were employed to provide patient isolation. Hospitals used lobbies, extra conference rooms, and Clinical Decision Units (closed units) among other spaces.

Negative pressure rooms are also normally in short supply. At least three hospitals used up their supply of negative pressure rooms at various points during the exercise. Again, hospital staff developed a number of alternatives to deal with the short supply including the use of spaces in radiology, same day surgery, the Endoscopy lab, and an off-site tent with negative pressure.

In addition, at least six hospitals contacted maintenance/facilities personnel to request additional reverse pressure rooms. Lastly, because both isolation and negative pressure rooms were in short

supply, at least eight hospitals placed their Pneumonic Plague patients in either isolation rooms or reverse pressure rooms.

Changeover to droplet isolation

As soon as the causative agent in a respiratory epidemic is determined, it should be possible to downgrade the isolation levels to droplet/contact precautions. The downgrading to the lower precaution level, however, did prove to be somewhat confusing and required confirmation. As seen in the following group of observations from May 13, 2003, one hospital took almost ten hours to be convinced; even after a number of checks, the Vice President for Medical Affairs had to convince the hospital ED staff that contact and droplet isolation was, in fact, sufficient.

- 1047: Nursing supervisor informed “we don’t need reverse flow. We’re assigning by unit for droplet and contact isolation,” as per the Vice President for Medical Affairs;
- 1138: Infection Control manager here—confusion about whether patients need to be in negative flow versus contact and droplet isolation from ED staff/medical doctor (MD); Infection Control Manager leaves to go to Control Center to verify;
- 1140: Call from Control Center—“Dr. says we don’t need reverse flow. We can do contact and droplet isolation” stated an ER Charge RN to staff/MDs in ED; and
- 2040: the Vice President for Medical Affairs clarified with ED staff/MD that reverse airflow isn’t needed—contact and droplet isolation is sufficient.

e. Resources: masks, and Personal Protective Equipment

The recent outbreak of SARS has also generated a great deal more emphasis on the importance of respiratory protection for patients and about higher levels of Personal Protective Equipment (PPE) for hospital personnel who come in contact with them. For an outbreak of Pneumonic Plague, masks are likely to represent an important means for infection control. During the FSE, the following hospital personnel were identified as potentially vulnerable to infection and thus required some form of droplet protection: doctors, nurses, triage and front line ED staff, X-ray technicians, security, registrar, and volunteers.

Figure 19 provides a breakdown of the various types of PPE worn by hospital personnel as noted during the exercise. Each category indicates, at a minimum, that particular pieces of equipment were being worn. The category *PPE* does not specify any one piece of equipment; the observations in this category likely range from masks up to mask, gown, goggles, and gloves worn by the staff member(s) being observed.

Figure 20 provides a breakdown of the various types of personal protective equipment worn by the exercise patients as noted during the exercise. The same categories were used for this plot as for Figure 19.

Both graphs note small, but important percentages of persons who were not wearing any masks. For the hospital personnel it is likely that this six percent is somewhat of an overestimate, because some notations in the data indicate staff and some notations call out a single individual. The patient number is a more reliable figure, since patients were not grouped using a similar

staff-like term. Regardless, it is important that the numbers in this category, whether hospital staff or patients, are as few as possible.

N-95 masks

During the exercise, both N-95 masks and surgical masks were used for PPE. Some EDs started the exercise using surgical masks then switched over to N-95 masks as the outbreak progressed. Others used the N-95 masks, but required some amount of additional instructions to use. One hospital was observed as having had all their nurses fitted for N-95s. The hospital also had adequate supplies of these masks throughout the exercise. Another hospital commented that not enough sizes were available. Other hospitals ran out and had some difficulty re-stocking. In DuPage County, it ultimately fell to DuPage County's EOC to coordinate a re-supply of masks to their county hospitals.

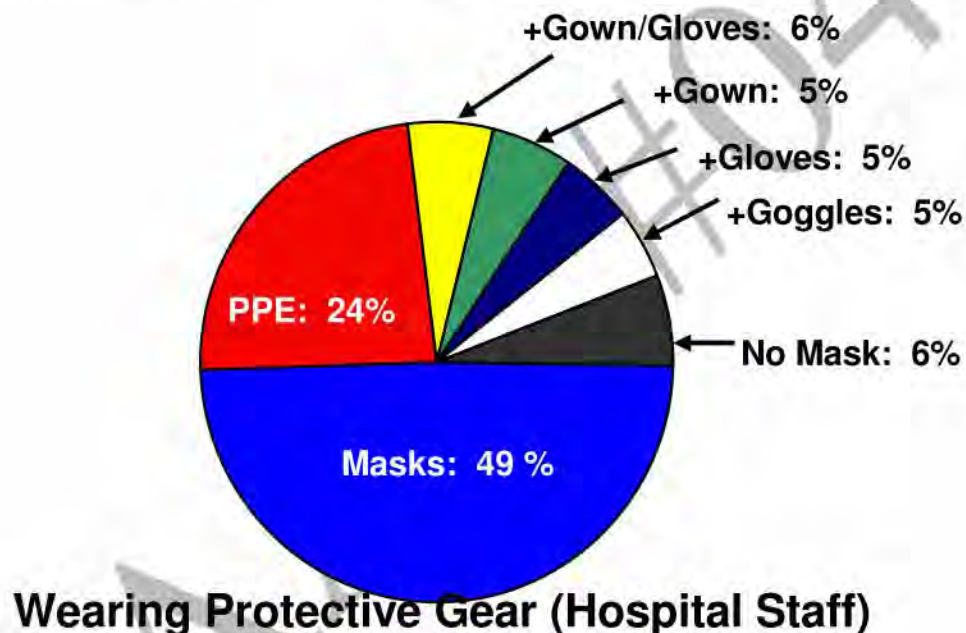


Figure 19. Wearing of Protective Gear by Hospital Staff (Clean Up?)



Figure 20. Wearing of Protective Gear (Exercise Patients)

f. Resources: handling of the dead

The FSE play included handling of the deceased and mortuary affairs. During the full five days of the exercise, 1,521 persons died as the result of the outbreak. Fewer exercise victims died during the three days of hospital play, but these casualties still stressed the morgue capacity for a number of participating hospitals. In fact, on the evening of May 13, 2003, three hospitals had reached their maximum morgue capacity.

Alternative morgues

A number of alternative morgue options were developed over the course of the exercise. These included other hospital sites (hospital garage, hospital barn, and a local ice rink) in addition to at least two different sizes of refrigerated trucks (truck capacity: 40 bodies; truck capacity: 108 bodies, based on exercise data).

These alternative morgues also required a morgue leader to set up and coordinate body storage and subsequent transport, as well as supplies such as body bags and duct tape. As part of this process, while such alternative morgues were being selected and established, temporary body storage was also provided for the hospital in the preliminary storage areas, which included:

- Increased stacking levels in the already full hospital morgue;
- Procedure Room;
- Urgent Care Area;
- ED; and
- Hazardous Materials Room

Some of these preliminary storage areas might have been refrigerated (one doctor ordered portable cooling units for this purpose) but the majority likely was not.

In DuPage County actual contact was made with the Union Pacific Railroad requesting refrigerated box cars to be used as temporary morgue facilities. Located immediately north of the county campus, the Union Pacific Railroad simulated the closing of a mainline track, and provided three refrigerated cars to expand the county's morgue capabilities.

Notifications/reporting of the dead

Deaths were counted and reported to the POD hospitals and then to IOHNO. This significantly increased the reporting requirements placed upon the hospitals. Along with a number of internal notifications, hospitals also sent this information to the County EOC, the County OEM, the Coroner, the Medical Examiner, the American Red Cross, the Funeral Director Association, and Funeral Homes (for the transport of non-infectious remains).

g. Antibiotics

Antibiotics were used as soon as the initial exercise patients arrived at hospitals. Figure 21 provides the percentage breakdown of antibiotics used to treat the patients throughout the three days of hospital play. The *Antibiotic* category includes all notations of *abx* in the data, where the data collector did not identify the specific prescription. The category *Other* consists of prescriptions of Chloramphenicol, Zithromax, and Amoxicillin, which were grouped for clarity. In addition to these prescriptions, eight percent of patients received two antibiotic prescriptions, primarily because medical personnel were suspicious of terrorism early in the exercise. Later in the exercise, two prescriptions were given because the centers for Disease Control and Prevention expressed concern that this strain of Pneumonic Plague may be resistant to traditional antibiotics.

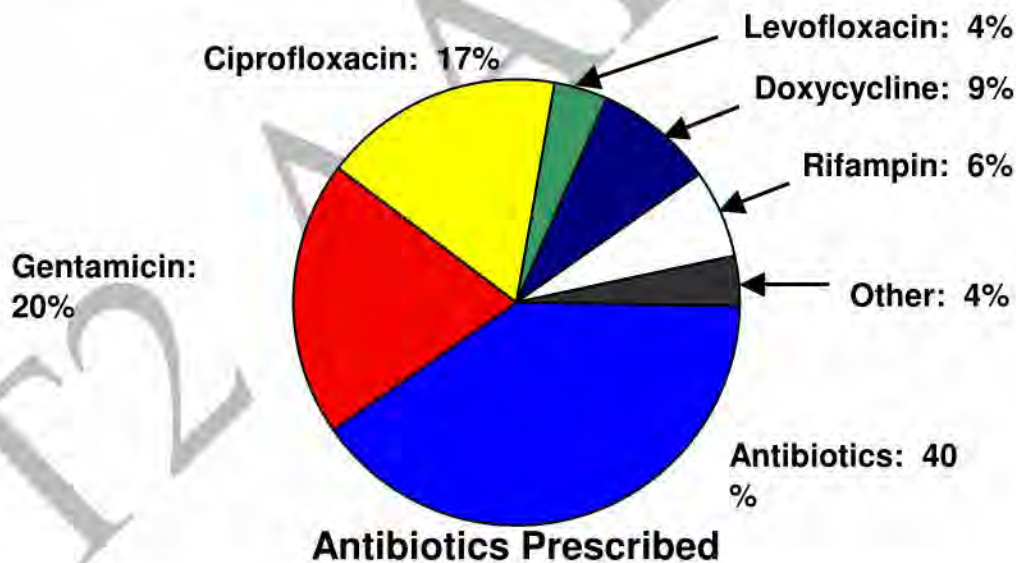


Figure 21. Antibiotics Prescribed during the Three Days of Hospital Play

In addition to both intravenous (IV) and oral antibiotics required for patients, hospitals provided either Ciprofloxacin or Doxycycline to their personnel once Pneumonic Plague was suspected and positively identified by IDPH. One hospital used Employee Health to manage the

distribution effort. Another hospital tasked Hospital Infection Control to determine the amounts of antibiotic supplies needed. A third tasked their Isolation Nurses with notifying the pool of personnel exposed prior to the discovery of the outbreak.

Per ED requests, hospital pharmacies determined the on-hand supplies of antibiotics for both patients and staff. For patients, stocks of the IV/oral supplies of Gentamicin, Streptomycin, Vancomycin, Ciprofloxacin, Levofloxacin, Chloramphenicol and Doxycycline were checked. Pharmacies were also tasked with additional orders of Ciprofloxacin and Doxycycline. In addition, at least one pharmacy was tasked to call the EOC to request the activation of the county's stockpile of antibiotics.

h. Additional space requirements

In addition to the previously mentioned requirement for additional beds, isolation rooms, reverse pressure rooms, and increased morgue capacity, and other space was voiced during T2. These needs also included additional space to triage patients, space to enable the ER to be segregated by plague patients versus non-plague patients, and a separate site to handle the worried-well.

Hospitals utilized various spaces to meet the additional triage requirements, including break rooms, hallways, the entrance outside the ED, pediatrics ER, minor care, and the catheterization lab. For the worried-well, at least one option considered was the helicopter hanger. The Family Medical Center department of at least one hospital was used for segregating the ER.

i. Ventilators

Responding to a large outbreak of a severe respiratory disease will require the use of respiratory support for the most critically ill patients. As was true with the other resources examined in this reconstruction, ventilator supplies were also counted and their numbers provided to POD hospitals and then IOHNO. On the morning of May 14, 2003, IOHNO requested additional ventilators from the Vendor Managed Inventory of the Strategic National Stockpile. This request was based upon patient number projections, not upon the number of ventilators currently in use at the time. During actual hospital play, in fact, the supply of ventilators appeared to remain adequate. Only one of the seven hospitals, for which ventilator data were available, indicated a need for more ventilators early on the evening of May 13, 2003.

4. Artificialities

Several artificialities or artifacts of exercise play affected the analysis of hospital play:

- Multiple reporting chains, the plethora of patient statistics available (reports from the media, control injects, the hospitals, etc.), and the number people in the reporting chain all complicated patient reporting. In many cases, individuals were able to obtain patient statistics from sources not anticipated or known by exercise control. During an actual event, patient counts would be generated through the reporting, not from the interaction of the reporting chain with exercise control;
- In a real event the reporting system would be more complex, with requirements to report on the evolution of the patient population as well as the general statistics (affected, dead, etc.);

- The Metropolitan Chicago Health Care Council (MCHC) injected additional, unscripted, patients into the exercise during the early phases of the exercise. These patients were intended to assist MCHC hospitals maintain their accreditation. However, these patients were inadvertently configured to resemble T2 FSE scripted patients, resulting in a distortion in the numbers of patients reported; and
- During the FSE, some media play was scripted. This meant that in some instances the reported patient numbers were based upon exercise injects, not the actual numbers of patients reported to decision-makers. One example of this type of reporting occurred with the Office of the Governor of Illinois. Ground truth patient counts had been given to the Governor prior to the start of the exercise. Using these numbers the Governor taped several interviews or reports incorporating those numbers. However, when they were broadcast, the ground truth numbers were significantly different from the patient numbers held by the State and local governments and public health authorities.

5. Conclusions

During a crisis like the one simulated in the Illinois venue, communicating data and information is critical to developing an accurate and comprehensive picture of what is happening. Communications require both a robust transmission system and sufficiently trained personnel to ensure that the communications occur and that the results are verified, then passed to the appropriate locations within the receiving organization. T2 illustrated the diversity and complexity of managing response resources in the public health and medical environment. With 64 hospitals, five POD hospitals, and three separate but interrelated statewide organizations (IDPH, IOHNO, IL State EOC) all collecting data and attempting to coordinate actions, information and data flow requirements became intense.

Hospitals and public health departments generally do not have the experience or the extra staff trained to handle large volumes of emergency communications. While personnel may be trained to operate particular fax or voice circuits, the existing infrastructure may not be adequate to sustain robust communications during a crisis of the type simulated during T2. Thus, as was the case in this exercise, problems develop when the system is activated.

During the FSE, the lack of a robust emergency communications infrastructure was manifest by a reliance on telephones and faxes for data transmission versus electronic transmission of data. It was also manifest in the loss of fax machines due to mechanical breakdown, inadequate staff to monitor them, or loss due to after-hour rooms that were locked. Likewise the lack of verified phone numbers for communications caused delays while emergency personnel looked for the correct numbers to report emergency data.

SUMMARY OF CONCLUSIONS— HOSPITAL PLAY IN THE ILLINOIS VENUE:

The T2 FSE exercised 64 hospitals in the Illinois venue making it one of the largest mass casualty exercise ever undertaken.

Hospitals still rely on telephones and faxes for data transmission vice electronic transmission. This manifested itself as a significant challenge during the FSE due to mechanical problems, inadequate staffing, and loss of data.

Hospitals should consider implementing a system in which data is entered digitally then transmitted electronically. This would eliminate many of the manual steps observed during the FSE and has the potential to minimize errors.

Because of the dual communications chains that exist, there is a need for organizations to coordinate the receipt and processing of information.

At the most basic level, it is possible to establish some principles for developing an effective emergency data communications system, which is essentially what was occurring as the hospitals reported syndromic, patient, and infrastructure information:

- Communications need to be robust and verifiable. It is critical that communications are being directed to the correct personnel or organizations (i.e., e-mail or telephone numbers must be correct) and that the receiving organizations received the right information. A record of the transmission is also required;
- Data should ideally be communicated over data lines, not voice or fax. Voice systems are good for person-to-person coordination (not necessarily organization to organization coordination), but neither voice nor fax are optimal ways to communicate numerical data. Using data communication techniques (e.g., e-mail, Internet transmission) leaves the data in machine-readable formats upon receipt;
- After they are generated, as few human hands as possible should touch data to minimize errors. For example, if information is copied down manually on a form, then the form is faxed (possibly degrading its readability) to a collection point, where it is then manually tabulated on another form, as is consistent with the IDPH emergency plan, and then entered into an information system for transmission, the potential for errors increases significantly; and
- Whether using data lines, voice, or fax, care must be made to ensure the security of the information being transmitted.

One way to overcome difficulties in the collection and reporting of data is to have data entered digitally at the point of origin, then transmitted electronically in digital form to all those who require the data. This would eliminate many of the manual steps currently involved in data generation at the hospital level, and provide for a more robust and verifiable set of data once it was received by one of the POD hospitals and IOHNO.

A larger issue, that was more difficult to document, was the movement of information within organizations once the information was obtained. The dual communications chain observed in the FSE, with the IDPH Infectious Disease Control receiving reports from local public health and IOHNO receiving reports from emergency departments at hospitals, is an example of the need for coordination within organizations for the receipt and processing of information.

The FSE resource requirements illustrated both the diversity of resource types required to respond to thousands of sick, dying, and dead, as well as the diversity of organizations looking for and providing resources. With 64 hospitals all looking for essentially the same set of resources, a wide range of potential solutions were developed to address the problem.

However, without adequate resource tracking it will be impossible to effectively allocate, expand, or acquire resources that address specific needs. Instead a general diffuse and untargeted effort to acquire resources will evolve as a result.

This page intentionally left blank

G. Decision-making under Conditions of Uncertainty: The Plague Outbreak in the Illinois Venue

1. Introduction

During a disease outbreak, whether naturally occurring or initiated through an act of terrorism, decision-makers must rely upon scientists, medical doctors, and the public health system for the information needed to make effective response decisions. Examples of such information include the progress of the disease, the behavior of the disease in various populations, and assessments of how the disease might be spreading. Often the early science on these questions is ambiguous or, in the case of historical diseases, open to various interpretations.⁹⁹

Decision-makers must work to formulate the right questions, and then interpret the answers within the context of the logistical, political, social, public health, and economic aspects of the response. This is difficult under the best of conditions, and made even more difficult during a terrorism response operation due to the enormous media and time pressures that decision-makers will be operating under.

The Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE) provided a unique environment that can be used to examine decision-making under conditions of information uncertainty. During the FSE, public health officials initially knew neither the extent nor duration of the terrorist-induced epidemic of Pneumonic Plague. These facts permit an examination of several questions related to decision-making under uncertainty, such as:

- How was the extent of the epidemic estimated;
- What were the estimates;
- What techniques were used to provide these estimates; and
- Did these estimates subsequently affect decisions (requests for resources, other teams, and capabilities)?

This *Special Topic* examines these questions in the context of events that occurred Illinois venue during the FSE. During the early phases of the exercise, participants were only seeing the tip of the iceberg in terms of the eventual numbers of patients that would develop. How they oriented themselves to the evolution of the disease and what impact that had on planning were aspects of the exercise in which science and policy-making interacted.

2. Background Pneumonic Plague

a. Defining the information iceberg problem

During the FSE, a simulated outbreak of Pneumonic Plague occurred in the Chicago metropolitan area. To illustrate the challenge of estimating the long-term consequences of the outbreak, the plot graph in Figure 22 shows the T2 scenario's patient population broken down into five potential pools: Not symptomatic, mildly ill, severely ill but not in a hospital, severely ill and in a hospital, and dead.

⁹⁹ Science: P. Anand; "Decision-making when Science is ambiguous" 8 March 2002, Volume 295, page 1839.

The plot shows the number of cases of Pneumonic Plague increasing along the negative y-axis, with time increasing along the positive x-axis. The figure is constructed this way to simulate a metaphorical iceberg, with $x = 0$ symbolizing the waterline. As the days of play continue from May 11 through May 14, 2003, only small fluctuations are seen in the number of persons diagnosed with plague. However, after May 14, 2003, the number of cases increases dramatically from less than 1,000 to more than 20,000.

This is termed the *information iceberg*, as the early presentation of the disease does not really foreshadow the potential size of the epidemic. The patients who present symptoms early in the epidemic are seen as the tip of the iceberg with their numbers appearing above the waterline, as they bring themselves into the hospitals for assessment and subsequent treatment. The remaining pool of patients remains under the waterline of the iceberg, where the graph ends on the last day of the exercise.

Understanding and successfully predicting the effect of the iceberg is critical to decision-makers. During the early stages of an outbreak, decision-makers are likely to see reports about only the early presenters, not the full number of exposed persons. It is absolutely critical to determine rapidly the scale of the outbreak. This is especially true in cases of potential bioterrorism where traditional epidemiological curves could be multiplied by multiple, continuing, or widespread initial exposures.

Public health officials, and other decision-makers, may determine the scope of the problem by employing epidemiological models based upon data reported by physicians, hospitals, and the public health infrastructure, as well as developing a clear understanding of the nature and transmission mechanisms of the disease; but they must also factor in additional assumptions in the case of bioterrorism.

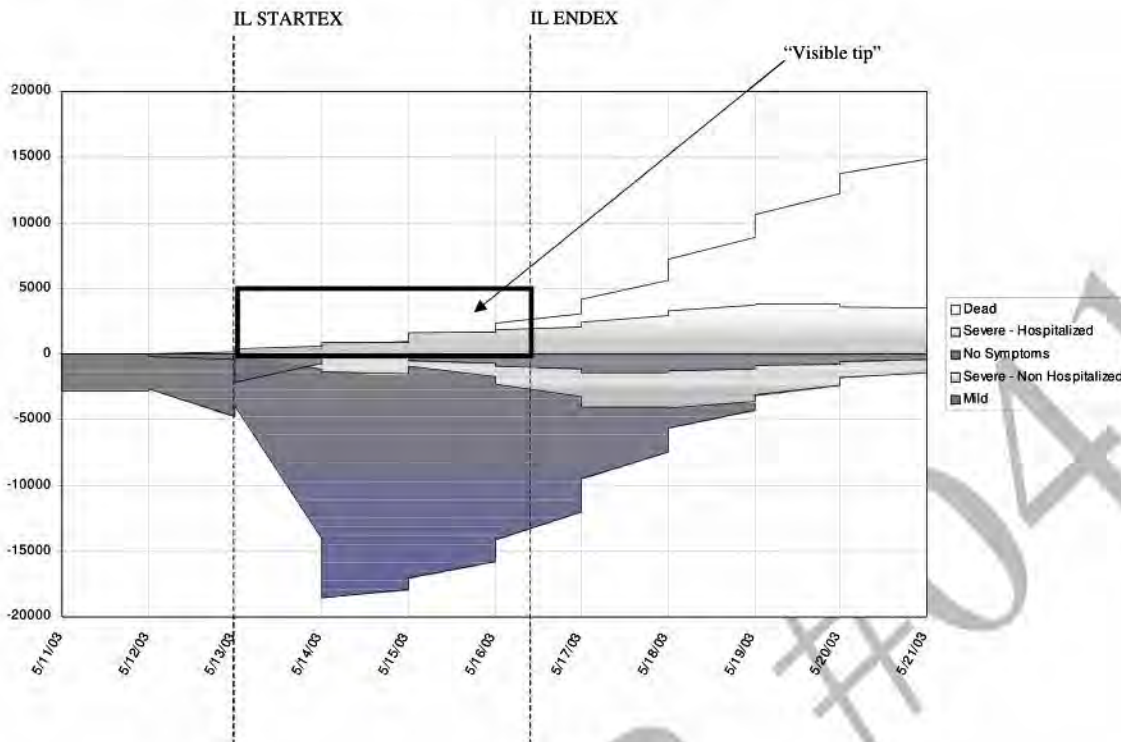


Figure 22. The Iceberg of Patient Population

b. Decisions using estimates and models***How do epidemiologists estimate the size and behavior of the disease***

A common approach for approximating these elements is to use models to estimate the progress of the disease. However, incorrect, incomplete, or inaccurate data or assumptions and information input to a good model can result in sub-optimal results for decision-makers. It is important for decision-makers to understand that even with good data, models are only an approximation of reality. In the case of a disease outbreak, data on the disease does not appear instantaneously at exactly the right time for decision-making. Instead it may be delayed and may contain inaccuracies. Mechanisms may not be in place to collect the right data in a timely fashion. Finally, the models themselves are approximations of the actual process by which diseases spread. It is also important to note that models are even less reliable when dealing with diseases like plague, particularly Pneumonic Plague for which there is a paucity of data. Additional complications occur with diseases that are deliberately introduced and optimized by terrorists to achieve high mortality and morbidity.

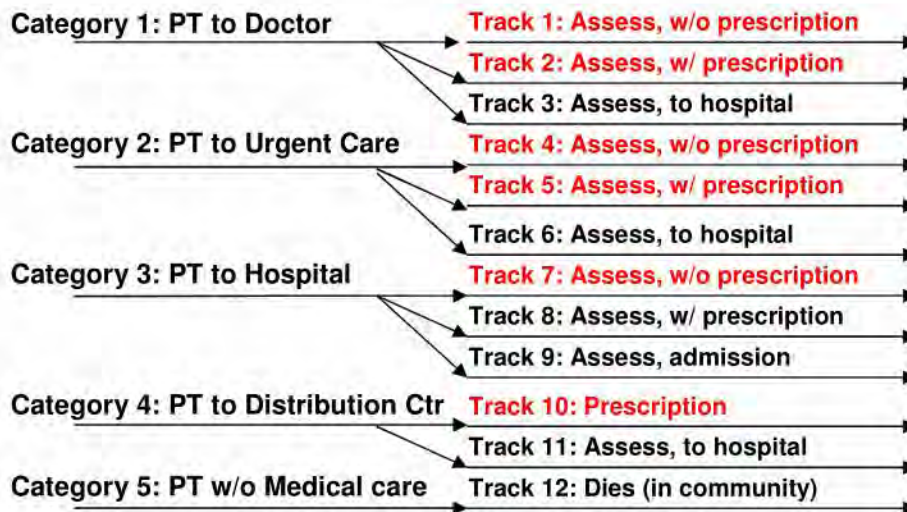
The estimates that models provide may well change over time as more data become available. A number of T2 After Action Conference (AAC) participants indicated “neither decision-makers nor the American public understands models and, in particular, won’t accept the fact that the answers keep changing.” Continuous changes in estimates can be disconcerting to decision-makers, and the general public.

c. T2 Chicago venue scenario and patient breakdown

The FSE Illinois patient population consisted of an initial group of 3,100 individuals exposed to Pneumonic Plague. This group would ultimately infect an additional secondary population of 18,434 persons. When exercise brevity (five days) is compared with the designed epidemic length (eleven days, from original exposure to D+9), the impacts of the 21,534 affected individuals were not fully explored.

The affected population design was initially divided into five separate categories: Not symptomatic, mildly ill, severely ill but not in a hospital, severely ill and in a hospital, and dead. Subsequent changes to this original design were accomplished in consultation with Illinois Department of Public Health (IDPH). These changes were designed to provide a reasonable representation of the responses individuals would have to becoming ill with Pneumonic Plague. The additional breakdown laid out twelve separate tracks that determined when the patients would arrive at hospitals, or if individual patients would avoid hospitals and seek medical care elsewhere or not at all. The breakout of these tracks is provided in Figure 23, which is color-coded to indicate those patients who would be captured as part of normal hospital reporting protocols. The red script indicates those infected individuals who would remain largely uncounted by the hospital system playing in the exercise but who would eventually require care nonetheless.

IL Patient Breakdown



Black = Counted by system Red = Not counted by system

Figure 23. Illinois Patient Breakdown

Figure 24 summarizes the number of victims who were infected (both the primary and secondary exposures) and those who would be so severely ill as to require hospital treatment for the days of the exercise.

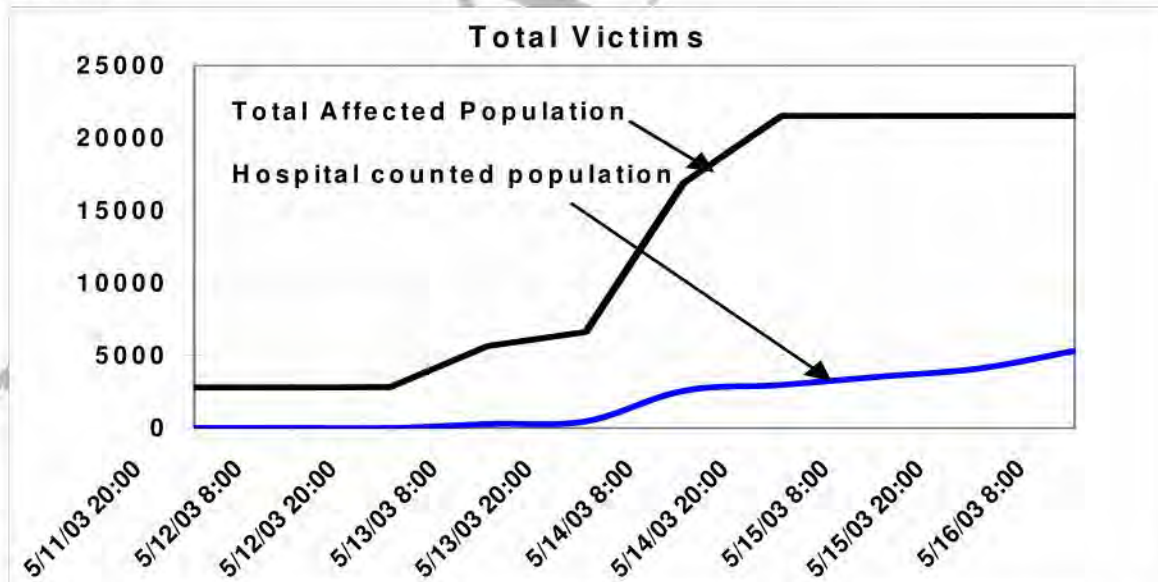


Figure 24. Total Exposed Population Compared With the Hospital-Counted Victims (All times Central Daylight Time (CDT))

3. Reconstruction (all times CDT)

a. How accurate was the data reported by hospitals

Patient counts reported by hospitals and physicians were lost during the exercise for a number of reasons. Patients may not have been counted because they did not report to hospitals or because the counts were corrupted somewhere along the way. This section discusses how information was lost to epidemiological modelers, public health officials, and other decision-makers during the exercise.

The data used to estimate the epidemic spread during the FSE suffered from three problems:

- Some data were simply not observed at the point of origin;
- If the data were observed, they may not have been reported accurately. For example, an accurate count of patients was incorrectly entered into a data reporting system; and
- The data may have been incorrectly defined. Even with accurate numbers, not all of the patients were placed in the correct category.

Figure 24 illustrates the problem of unavailable data: Some patients were not entered into any data system. These patients could not be added to any hospital patient counts because they either never went to a hospital or they were released upon assessment in the Emergency Department (ED) and not counted.

Table 8 summarizes the percent of victims who were eventually seen at hospitals but who remained out in the community until they received treatment at hospitals or from their doctors, or died from the disease. At the end of the exercise, approximately seventy-five percent of the exposed population remained unseen because they had not yet become more than mildly symptomatic.

Table 8. Percent of Infected Population Seen in Hospitals by Exercise Date/Time

TIME	TOTAL SEEN	TOTAL INFECTED	%
13 May 0800	283	5656	5
13 May 2000	460	6634	6.9
14 May 0800	2566	16885	15.2
14 May 2000	2977	21534	13.8
15 May 0800	3546	21534	16.5
15 May 2000	4084	21534	19.0
16 May 0800	5322	21534	24.7

Inaccurately reported data can be detected by comparing patient numbers reported and logged at the Illinois Venue Control Cell (VCC) with the ground truth scenario patient population. The patient data for the 1700 - 2400 timeframe on May 12, 2003,¹⁰⁰ is provided in Table 9. The numbers vary considerably from the ground truth, depending upon which source is consulted

¹⁰⁰ This is the time period during the exercise where the Metropolitan Chicago Health Care Council did not inject additional patients into the patient population.

(both hospital patient numbers and public health numbers were logged on VCC wall charts and the VCC controller log has also been reviewed).

As can be seen in Table 9, none of the logs of patient counts maintained by the VCC agreed completely with the ground truth patient numbers from the scenario. This may be the result of the complex way in which patient data was exchanged. Communications took place over fax, landlines, and cell phones. This led to a number of ways to log the data as well as a variety of different people reporting the data. Variance in the reporting source and the method of reporting probably represents part of the reason why patient counts vary.

It is also important to note that the 1700 - 2400 timeframe on May 12, 2003, represents data from the earliest part of the exercise. After this time, patient numbers climbed considerably. If reporting wasn't accurate early on, during a low volume of patients, it might be expected to lag behind actual counts under the more stressful conditions of higher patient volumes. Unfortunately, due to the problems encountered with patient numbers later in the exercise, it was not possible to determine whether the variance in patient counts actually increased as the exercise progressed.

Table 9. Reported Patient Numbers Logged at VCC as Compared to Actual Scenario Numbers (May 12, 1700 - 2400)

CITY/ COUNTY	HOSPITAL PATIENTS (GROUND TRUTH)	HOSPITAL PATIENTS LOGGED: VCC CHART	HOSPITAL PATIENTS LOGGED: VCC LOG	PUBLIC HEALTH (GROUND TRUTH)	PUBLIC HEALTH LOGGED: VCC CHART	HOSPITAL DEATHS (GROUND TRUTH)	DEATHS LOGGED: VCC CHART
Chicago	22	11	9	10	5	0	0
COOK	38	26	15	29	26	2	0
DuPage	19	0	5	16	5	1	0
Kane	10	6	0	9	6	0	0
Lake	13	0	0	12	0	1	0
TOTALS	102	43	29	76	42	4	0

Another reason why the counts in Table 9 do not match is that the definitions of what was being reported do not necessarily match. As noted earlier, the ground truth scenario divided the patients into pools of those who would visit the emergency department (ED), those would subsequently be admitted, those patients sent to the emergency room by their doctor or by

another medical facility, and the dead. These specific definitions, however, were not adhered to by reporting hospital personnel and resulted in patient reports that, while counted in the totals, would not have accurately reflected the scenario.

b. Estimating the course and scale of the epidemic

During the FSE, participants used a number of approaches to produce estimates of the Pneumonic Plague epidemic. The results of these efforts helped determine strategies for antibiotic distribution, the need for additional antibiotics from the Vendor Managed Inventory, and the need to identify additional sites for patient treatment and handling of the dead. It should be noted that in the case of a terrorism attack, the progress of the disease would likely exceed that which would be encountered in a natural outbreak, suggesting that decision-making would need to be guided by a broader understanding of the threat environment.

The following sections describe several of the different approaches that were used to estimate the affected population during the FSE. These approaches are compared to the ground truth numbers for patient counts in the scenario, not for the purposes of critiquing them, but to indicate the ways organizations approached these types of problems.

Example 1 (Patient estimate). Illinois Operational Headquarters and Notification Office

Based upon the reported patient numbers at 1600 on May 13, 2003, (338 cases, 154 dead)¹⁰¹, Illinois Operational Headquarters and Notification Office (IOHNO) personnel used a simple approach to estimate the numbers that might be presented to their hospitals over the next few days of the exercise. They chose a multiplicative factor (initially 5-6). This factor was a means to estimate how many additional cases each initial case could produce. This resulted in an estimate of 2,000 cases with 1,000 dead for a total of roughly 3,000 affected persons. The multiplicative factor was almost immediately doubled, producing estimates of 4,000 cases with 2,000 dead, for a total of 6,000 affected individuals.

The factor was doubled because IOHNO felt that the patient numbers were being significantly underreported. It is interesting to note that this rough estimate was within fifteen percent of the final actual total patient population at 1200 on May 16, 2003, (5,349 cases, 1,521 dead, total of 6,870), which overestimated the dead and underestimated the survivors.

Because the State of Illinois has a total of 8,263 beds statewide, some of which would be not be used for plague patients, this IOHNO estimate suggested that hospital facilities would be severely strained by downstream patient numbers. More significantly, this estimate was used to request two Disaster Medical Assistance Teams and one Disaster Mortuary Operational Response Team. IOHNO's approach depended heavily upon the expertise of those making the estimates.

¹⁰¹ Note that this is out of the range of the May 12, 2003, data presented in Table 9. However, as was argued in the previous section, inaccurate early data counts are likely indicators of inaccurate counts throughout the exercise period. Thus, it is likely that these initial numbers, and all those quoted in these examples, differ from ground truth by an unknown but significant amount.

Example 2 (Patient estimate). Data obtained from the Chicago-area FEMA Regional Operations Center

Data from the Chicago-area FEMA Regional Operations Center (ROC) indicated that an estimate of the epidemic was provided during a briefing on May 16, 2003. The graph shown in Figure 25 is a copy of the graph used in the ROC. The numbers used were those reported by the IDPH.

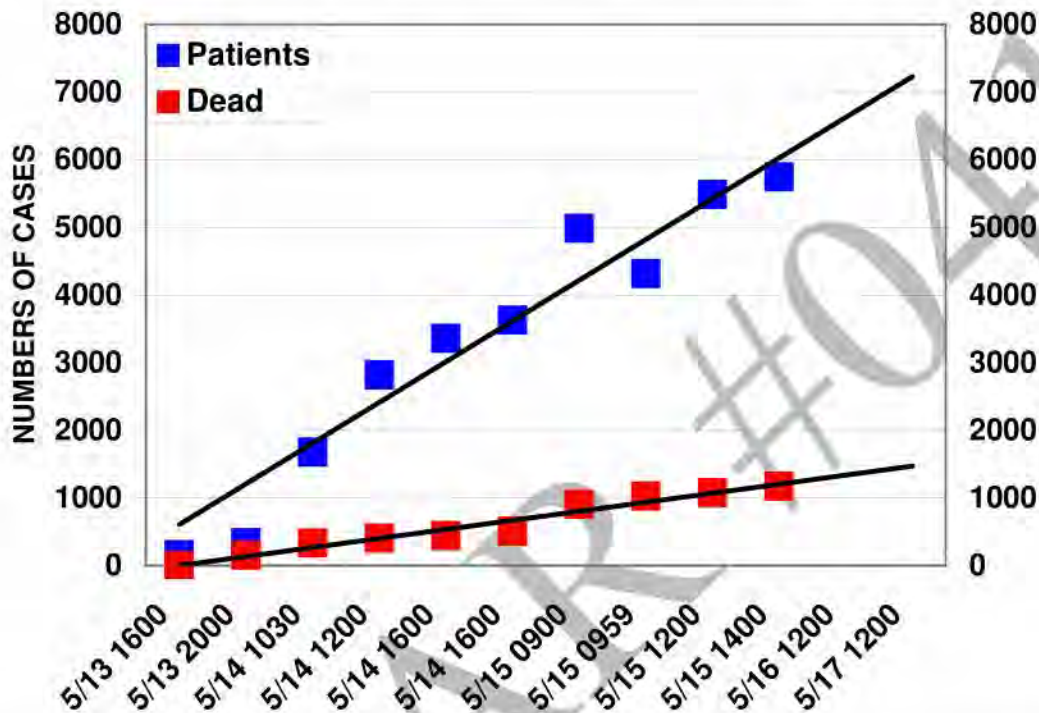


Figure 25. Chicago-area FEMA ROC Patient and Dead Estimates A significant problem is apparent from an examination of this graph. The data on the x-time axis are plotted at equal intervals. However, the actual time intervals on the plot are not equal even though they are portrayed that way. As a result, the straight line fit through the data is incorrect. Once the data are correctly plotted with respect to time (see figure 26), they are more correctly seen as clustered groups of data, not equally spaced in time.

The plot in Figure 26 indicates a patient population of 8,200 at 1200 on May 16, 2003, that would increase to 11,000 persons on May 17, 2003, (compared to 7,200 in the previous figure). Similarly, the estimates of the dead, 1,700 increasing to 2,200 on May 17, 2003, are significantly different than the original estimates shown in figure 25. In fact, if the estimates in figure 25 had been used, they would have underestimated both the patients and dead by approximately fifty percent for May 17, 2003, the day following the conclusion of the exercise. While this approach overestimates the number of sick and dead patients compared to ground truth at 1200 on May 16, 2003, it does give a better sense of the developing scale of the outbreak that would have become apparent if the exercise had continued passed May 16, 2003.

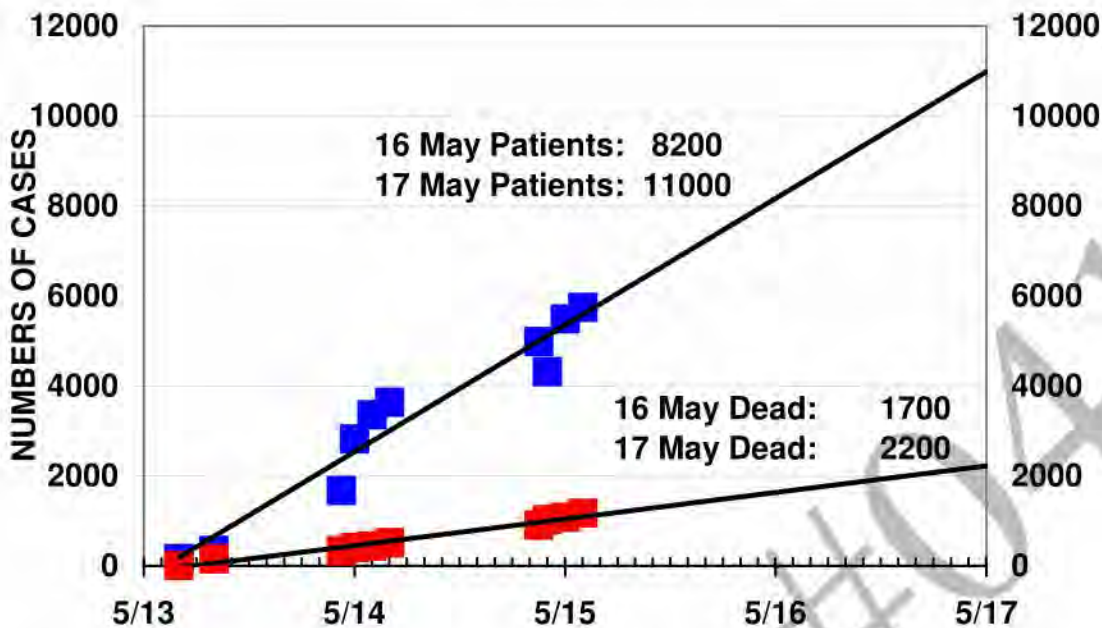


Figure 26. Correct Plot of Patient Numbers and Dead Numbers Versus Time

Example 3. DuPage County Emergency operations Center

The DuPage County Emergency Operations Center (EOC) called in a Geographic Information Systems (GIS) analyst to help estimate the number of DuPage County citizens who could have been at each of the three release sites in the Chicago area. The EOC suggested that this information could provide some indicators of which Strategic National Stockpile (SNS) distribution sites (located around the county) might be busiest and which hospitals might be seeing more patients. The first set of estimates was based upon raw numbers of people from specific areas of the county who were at the United Center during the Saturday night game. The GIS analyst got this information from the United Center ticket box office based upon zip codes. Next, the analyst collected data for the numbers of county resident who ride the single train line coming out of Union Station that passes through DuPage County. The analyst used the average Saturday traffic on that line and counted the number of people who got off at each station in the county.

DuPage County accounted for one percent of the people who attended the hockey game and for fifty-two percent of the people who left Union Station via the train line. Estimates of DuPage County–O’Hare traffic were not developed because of limited time and the greater number of variables. An estimated seventeen percent of the total people infected at the first two sites were from DuPage County. Following his presentation to the EOC, the DuPage County Office of Emergency Management said that while GIS is not usually tapped in an emergency response, that would have to change based upon how seemingly valuable their skills and data could be.

The final report by the DuPage count analyst discussed the methods and results and is quoted here in full:

During the exercise, it came to light that the State of Illinois pharmaceutical supply was limited, and we needed to identify the approximate number of DuPage County residents exposed to the biological releases and what portion of the county they reside.

There were three biological releases in the City of Chicago; Union Station (released 8:00 am, United Center (during a Blackhawk's playoff game), and O'Hare International Airport (International wing)

For the Union Station data collected we asked Metra to provide us with train ridership information on the Burlington Northern Line for the total trips leaving Union Station to DuPage County on an average Saturday. Metra provided the totals as well as the breakdown per train station in DuPage County. The Burlington Northern Line is also the only commuter line in DuPage County that leaves from Union Station.

The United Center data was provided by the Blackhawk's Director of Ticket Operations. The data reflected the last game of the season, a month prior to TopOff2, and was a sold out event. This event would provide us with the most accurate information we could have hoped possible. The attendance count was provided to us for each zip code contained in DuPage County.

Information was not available for O'Hare International Airport in the time frame available.

These numbers were tabulated and mapped out displaying the concentrations of potentially infected residents.

These estimates were calculated to provide the State of Illinois with a percentage of potentially infected residents so DuPage County would receive the bare minimum amount of pharmaceuticals from the underestimated Illinois stockpile.

The data gathered here reflects DuPage County residents only. Intended to provide rough estimates for pharmaceutical acquisition, and to provide a general overview of the concentrated areas in DuPage County. For an actual statistical analysis, this information would have been passed along to an epidemiologist for rate of spread calculations and probability modeling. A 3 hour window was given for data collection, tabulation, and display.

Given the parameters analyzed—the final estimate of the total exposed population, of which nineteen percent would have been DuPage County residents—was 25,706 persons. The actual scenario numbers totaled 21,534 persons, 3,100 in the initial population and 18,434 in the secondary population. The advantage to this approach was that it avoided all the significant problems in the patient population data and, in addition, provided an estimate not based upon projections, merely on normal use data—which is likely to be a better data set, unaffected by either exercise play or unannounced real-world attacks.

Other efforts

In addition to the efforts described above, two other efforts were identified that attempted to model the epidemic spread. There were also isolated events where decision-makers attempted to deal with the uncertainty involved in the response. This section covers all of these isolated events.

Statements were made at the T2 AAC that indicated the Illinois Crisis Action Team (IL-CAT) modeled the epidemic. Further information about the results of this modeling is not available, as the data collectors in the Joint Operations Center did not capture it.

The Centers for Disease Control and Prevention (CDC) apparently also estimated the scope of the epidemic on the second or third day of the exercise. At the AAC, it was reported that the CDC modeled the epidemic using the number of reported cases (from IDPH), the known incubation period (two to seven days, normally two to three days), and a rate of transmission of three secondary cases per primary case. In actuality, the rate of transmission used in the scenario depended upon the site of exposure: seven secondary cases per primary case at the United Center and eight secondary cases per primary case at Union Station and O'Hare International Airport.

Unfortunately additional data were unavailable to the evaluation team other than what was discussed at the AAC. Thus at the time of preparation of this draft report, there is no indication about the methods used, the results obtained, or whether decisions were made based upon the information. The report indicated, however, that the resulting predictions were within approximately ten percent of the final patient numbers.

In addition to modeling the epidemic outbreak, other estimates were made by officials. These "back of the envelope" calculations were important in several decisions, particularly for decisions regarding resource allocation.

At 0915 on May 14, 2003, the Chicago DPH determined that the SNS would be distributed according to the city's and county's population. The initial planned distributions were: Chicago—12,400 doses; Cook—12,500 doses (6,250 Doxycycline, 6,250 Ciprofloxacin); DuPage—10,100; Lake—6,000; Kane—4,400.

The reason that public health officials decided to distribute according to population, versus actual number of cases, was they lacked confidence in the accuracy of the number of cases being reported. Likewise they did not have a clear understanding of how many patients would ultimately be affected in each county. They did, however, know how many potentially affected persons lived in each county and saw that as a way to estimate the vulnerable population versus the infected or exposed population.

On May 14, 2003, Cook County DPH needed to know how many persons working at hospitals in Cook County would need prophylaxis. Instead of attempting to determine the potentially exposed population at each of the 22 county hospitals, Cook County DPH simply took the two largest Cook County hospitals, averaged the number of persons who would need prophylaxis, and then applied these numbers to the rest of the 22 hospitals. This over-estimated the need for prophylaxis, but resulted in a quick answer that would allow the prophylaxis to be distributed.

4. Artificialities

Several artificialities affected the analysis of this subject:

- The Metropolitan Chicago Health Care Council injected additional, unscripted, patients during the early phases of the exercise. These patients were intended to assist hospital accreditation. However, they were inadvertently configured to resemble T2 scripted patients, resulting in a distortion in the numbers of patients being reported. Because these patient numbers were not recorded, it complicates an understanding of how patient counts and epidemiological models played into the scenario; and
- During the exercise some media play was scripted. This meant that some patient numbers were reported based upon exercise injects, not the actual numbers of patients being reported to decision-makers. One example of this type of reporting occurred with the Office of the Governor of Illinois. Ground truth patient counts had been given to the Governor prior to the start of the exercise due to an exercise artificiality necessitating the pre-taping of top official statements. Using these numbers, the Governor taped several interviews or reports incorporating those numbers. However, when they were broadcast, the ground truth numbers were significantly different from the patient numbers held by the State and local governments and public health authorities.

5. Analysis

During the FSE there was significant uncertainty in the patient numbers. Indeed some of the artificialities discussed in the previous section may have increased the uncertainty. While the artificialities were unrealistic, the chaotic and uncertain environment they produced was realistic.

Decision-makers and those attempting to estimate the exposed population reacted in a variety of ways to the problem of uncertainty in the patient numbers. The methods used by the DuPage County GIS analyst attempted to resolve the fundamental conflict they were facing which was that the patient data were potentially inaccurate but that they needed accurate predictions of the number of infected persons in the county. By knowing the day, time, and place of the release and combining this information with demographic, economic, medical, and law enforcement data, the analyst was able to make a reasonably accurate estimate without knowing the detailed progression of the actual cases of the disease. Participants who chose to use the actual numbers of reported cases could be said to be ignoring the uncertainty inherent in the data. Even if they knew that the data were suspect, they still used them, as there was no other apparent alternative. In these examples, reported caseloads were used in various approaches to develop an estimate of how many patients would need treatment.

Finally, some participants focused on other measures in order to move decisions forward. For example, the Chicago DPH decision-makers lacked confidence in both the data they were receiving and their ability to use the data to predict how to allocate resources. Instead they focused their decision upon the vulnerable population, instead of focusing on the infected or exposed populations.

6. Conclusions

This section provides three sets of observations and conclusions: 1) one relating to uncertainty and how participants dealt with it, 2) the information iceberg problem, and 3) a more general set of observations of how epidemiology played in the various EOC operations.

a. Uncertainty

From the preceding reconstruction, the following was observed:

- Uncertainty in the patient population numbers existed during the FSE. Most of this uncertainty was due to exercise artificialities, but it is not clear that during a real event the magnitude of the uncertainty would be less, even if the causes were different; and
- It is not the fact of uncertainty that affected exercise decision-making but how participants dealt with the uncertainty. By finding data, systems, and methods that allowed them to work around the problems with patient reporting data, some participants were able to deal with the uncertainty and make informed decisions.

b. The information iceberg

There were apparently few attempts to understand the long-range patient load. It is unclear why so few attempts were made. Two possible reasons include:

- Lack of long-term exercise play. Participants may have simply ignored what they did not need to worry about; and
- Lack of confidence in the patient data, and no clear way to model the long-term effects in the face of poor patient data.

The last reason may be the most important for developing a general lesson learned about the iceberg problem. The DuPage County GIS analysis was the only documented effort that examined how large the problem might be. This analysis was not accomplished using patient data but rather relied on an estimate of the number of people who might be exposed in the county.

Finally, decision-makers should be knowledgeable of the information iceberg problem for contagious diseases such as plague and especially in cases of potential bioterrorism. It is important for them to expect it, look for it, and question their advisors when it is not brought to their attention.

SUMMARY OF CONCLUSIONS— DECISION-MAKING:

The extent of the affected population will always be uncertain in a bioterrorism incident. Public health officials and decision-makers use epidemiological models, informed by the threat environment, to help determine the scope of the problem.

During the FSE, few attempts were made to understand the affected population. *The DuPage County GIS analysis was the only documented effort that examined how large the problem might be.*

To alleviate some of the inherent uncertainty, model predictions and patient data should be coordinated among agencies and across jurisdictions. In addition, data collection should be better executed than was observed during the FSE.

By finding data, systems, and methods that allowed them to work around the uncertainty, some officials were able to make more informed decisions.

c. Other issues

These is a set of observations that arose from the work discussed here, but do not relate to either the problem of uncertainty or the epidemic profile.

Information sharing

Once model predictions and patient data are acquired they should be shared with everyone involved in the operation. In fact, information about some modeling efforts was only shared among all the participants during the AAC. There is no evidence that any of the results of these models were provided to other operations centers during the FSE.

The DuPage County EOC felt it would have benefited from model predictions by using them to predict the requirements for and deployment of ambulances throughout the county. A senior DuPage County EOC watch-stander noted (speaking to a member of the Illinois CAT during the AAC), “Why didn’t I know that those predictions were available?”

Data collection.

One way to reduce uncertainty and improve the overall fidelity of the data is to do a better job of collecting it. There are systems available, such as the State of Illinois’ Phase I and Phase II disaster reporting system, which could be used to collect patient data as well. This system collects bed counts, ventilators, blood supplies, among other supplies, during a disaster. However, the accurate collection of even the existing data requires considerable numbers of personnel, personnel that may not be available during an emergency.

This page intentionally left blank

H. Balancing the Safety of First Responders and the Rescue of Victims

1. Introduction



Historically, first responder rescue agencies have demonstrated high competency and experiential knowledge in managing traditional rescue situations: natural disasters, fires, and technical rescue challenges. In the hazardous materials (HAZMAT) environment, hazard identification is assisted by placard systems, knowledge of shipping contents, pre-planning at fixed facilities, and field-testing processes to identify common hazardous substances. In such incidents when victim survival is dependent upon timeliness of medical treatment (referred to as the *golden hour*), first responders are typically attempt to initiate rescue and removal of victims as rapidly as possible, while Incident Commanders manage responder safety with an ongoing risk-benefit analysis.

However, when faced with a potential weapons of mass destruction (WMD) emergency, first responders encounter a greater risk of becoming casualties themselves. For example, in Top Officials (TOPOFF) 2000, the first responders to arrive after the explosion in Portsmouth, New Hampshire, were incapacitated by a persistent chemical agent used in the attack. During the 9/11 World Trade Center attack, many New York City police and fire fighters died when the towers collapsed. In addition, first responders may be faced with delayed identification of toxic substances, the potential existence of secondary explosive devices, and other unknowns. Under these conditions of additional danger and uncertainty, consideration of risks and benefits in the development of action plans becomes more challenging. If victims are in immediate need of rescue, the initial action plan may reflect best guess/best practices information, placing responders in a rescue mode. However, as more information becomes available, plans can change and rescue operations may come to a halt. This is the scenario that was observed at the Seattle radiological dispersal device (RDD) site during the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE).

During the FSE, a number of public health officials and data collectors at the incident site, many of whom were subject matter experts (SMEs), expressed concern about the time it took to triage, treat, and transport victims. Commentators on the Virtual News Network (VNN) also raised this concern. Given the uncertainty surrounding the explosion, particularly when many of the responders artificially had the knowledge that it was a radiological incident, the Incident Commander had to take precautions to ensure that the responders were safe. This *Special Topic* focuses on the issues surrounding the balance of responder safety and victim rescue.

2. Background

a. Interagency communication

In large-scale incidents and exercises, communication between agencies is typically the largest command and control challenge. Command decision-making and development of an integrated

incident action plan are enhanced by effective communication links between the various agencies on the ground. The ability of a local Incident Commander to use information (e.g., radiation exposure levels, plume modeling, and toxic agent identification) provided by State and Federal responders depends on rapid and effective communication. With more detailed information, the incident action plan and the related risk-benefit analysis evolves with increasingly greater accuracy.

During the 9/11 terrorist attack on the Pentagon, the Arlington County (Virginia) Fire Chief managed his resources on the scene with a number of local and Federal agencies. He stated, "They [the other agencies] understood their role, which was to help the fire department move the incident through its various phases."¹⁰² Avoiding duplication of effort, the Arlington County Fire Chief put the Federal responders to work assisting the Fire Department. For example, he used Federal resources to set up chain-link fencing and scene security in order to isolate the scene. These types of decisions allowed local and Federal agencies to work together and solve incident problems rapidly. He also stated, "Having a relationship with key officials prior to the incident does make a difference. We worked regularly with our military personnel, our Federal Bureau of Investigation (FBI) and Federal Emergency Management Agency (FEMA) personnel. You have to work on those relationships before the incident, not during the incident."¹⁰³

b. Risk-benefit analysis

The use of risk-benefit analysis is common in first responder incident command systems for routine responses, and is likely even more necessary when responding to a possible terrorism event. With the potential use of WMD and secondary explosive devices, it is imperative to maximize the safety of first responders to avoid having them become victims themselves.

Fire departments typically maintain a definite posture towards life safety and rescue. For example, Montgomery County (Maryland) Fire Rescue (MCFR) has a systematic approach to risk-benefit analysis. Their policy states, "Saving live victims is the rescue mission, while minimizing the risk of harm to the rescuers."¹⁰⁴ This does not mean that fire and rescue operations are suspended until all possible risks are defined in detail; the objective of the first responders remains saving as many lives as possible. In the event of a chemical attack, MCFR policy cautions first responders "not to 'automatically' assume that the incident involves super toxic chemical agents."¹⁰⁵ For the Phoenix Fire Department (PFD), risk-benefit analysis means that when victims are present all first responders are to move forward with standard operating procedures unless a secondary device is present. However, if no apparent victims, life hazards, rescue situations, or threatening fires exist, fire department personnel should not be exposed to risk. PFD policy states that in this situation "first arriving units should secure a perimeter, evaluate the situation, and await the arrival of the Hazardous Materials Technicians."¹⁰⁶

¹⁰² Elliott, Timonhy. "First Responders, Feds Join Forces." *Fire Chief*. December 2001. Fire Chief Magazine. July 8, 2003.

¹⁰³ Ibid.

¹⁰⁴ Montgomery County. Montgomery County, Maryland Fire and Rescue Service. *Managing the Consequences of a Chemical Attack: A Systematic Approach to Rescue Operations*. Montgomery County: Maryland, 2001.

¹⁰⁵ Ibid.

¹⁰⁶ City of Phoenix. Phoenix Regional Standard Operating Procedures. *Hazardous Materials Weapons of Mass Destruction Chemical, Biological, Radiological*. Phoenix: Arizona, 2000.

The first step in conducting a risk-benefit analysis involves assessing the disaster scene and gathering vital information. The early stage of information collection can include field reconnaissance (recon). Initial recon is viewed as a key factor when deciding if the rescue is a “Go” or “No-Go” situation. Ongoing data collection through recon provides the Incident Commander with the information needed to make accurate decisions regarding risk and resources. In a presumed WMD situation, the recon team is not sent to help victims; instead, their mission is to establish how many victims, the type of incident, and the level of risk involved with the incident. This information helps guide commanders in determining how to address the incident, and best save lives. However, it also means that the response time to triage, treat, and transport is necessarily longer than during a non-WMD incident.

c. Personal Protective Equipment

A significant component of an initial action plan is the determination of appropriate Personal Protective Equipment (PPE) for responders. Because time, distance, and shielding are important means for protecting responders from the exposure to gamma radiation, training is also a necessary pre-cursor to the response to incidents involving radiation.

The recon team is the first to move into an operational area. Therefore, it is imperative that they are equipped to handle any level of risk so that they can safely report back to the command post. MCFR policy is that the recon team wears the best available protective clothing with standard firefighting breathing apparatus:

For initial on-scene quick rescue of live victims, first responders should wear their turnout gear, self-contained breathing apparatus (SCBA), and butyl gloves. However, later into the incident and where rescue may still be required, first responders should wear Level B Protection or the appropriate chemical suit as indicated by the site safety plan.¹⁰⁷

The Boston Fire Department has similar guidelines regarding PPE. When Boston’s first responders arrive on the scene of a presumed chemical attack, guidelines require them to don all PPE equipment available before entering the contaminated site.¹⁰⁸

There has been much controversy on the best way to protect response units, especially when dealing with unknown agents in the opening hours of a response. In 1999, the Soldier and Biological Chemical Command (SBCCOM) issued guidelines for Incident Commanders’ usage of PPE. While some departments felt these guidelines were useful, more than half of the fire service survey respondents said they would not sanction SBCCOM guidelines and would have developed their own PPE guidelines.¹⁰⁹ Some departments, including MCFR, have adopted selected SBCCOM techniques into their own guidelines. For example, MCFR instituted the usage of portable fans to help ventilate buildings where chemical agents may be present.^{110,111}

¹⁰⁷ Montgomery County. Montgomery County, Maryland Fire and Rescue Service. Managing the Consequences of a Chemical Attack: A Systematic Approach to Rescue Operations. Montgomery County: Maryland, 2001.

¹⁰⁸ City of Boston. Standard Operating Procedure No. 61. Operations and Response to Terrorist Incidents. Boston: Massachusetts.

¹⁰⁹ Peterson, David F. “Terrorism and Turnouts: The Controversy.” Fire Engineering. March 2002. Fire Engineering Magazine.

¹¹⁰ SBCCOM test results showed that 50-70% of chemical concentration can be decreased when the portable fans are used.

Specialized protective equipment matched to hazardous substances is ideal but is currently not likely to be available in a timely manner or in quantity enough to accomplish victim rescues in most hazardous environments.

d. Secondary explosive devices

Terrorists can employ a number of tactics to inflict as much damage as possible. One strategy used by terrorists is the use of a delayed secondary explosive device. The purpose of such a device is to injure or kill first responders. Typically, these devices are hidden near the original incident.

Secondary explosive device awareness has become policy and is accounted for during first responder training throughout the world. Most first responder units understand the need to watch out for these devices. A review of several fire rescue policies indicates that even if secondary explosive devices are suspected, rapid intervention and victim removal still remains the ultimate goal. If secondary devices are found, response units are directed to immediately pull back and wait for specialized explosive ordinance disposal assets. For example, the PFD has a simple yet precise procedure addressing awareness of such devices. The first arriving units are expected to establish command and begin sizing up the situation. While responding, they are to:

...be aware of secondary devices designed to injure additional victims and/or first responders. Upon sighting a device that appears operable, [personnel are instructed to withdraw] until Police Bomb Squad has inspected/rendered safe any suspicious appearing device.¹¹²

MCFR and the Denver Fire Department both have similar response methods.^{113,114}

It is also useful to examine the emergency response policies of Northern Ireland and England. Their use of incident command and risk-benefit analysis has proven successful over decades of domestic terrorism response experience. The Northern Ireland Fire Brigade maintains an awareness of potential secondary device placement, avoiding command post locations near dumpsters and parked cars, where such devices may be hidden. Arriving bomb technicians sweep the command post areas first, eliminating the possibility of additional explosives.¹¹⁵ The *United Kingdom Home Office Strategic National Guidance* also emphasizes the need to sweep command post and support areas for the presence of secondary devices.¹¹⁶

3. Reconstruction

The evaluation team did not obtain specific data describing the incident commander's risk-benefit analysis process. However, it did obtain data describing the response, which is the focus of this reconstruction. Figure 27 depicts a timeline of the key events during the rescue phase at

¹¹¹ Montgomery County. Montgomery County, Maryland Fire and Rescue Service. *Managing the Consequences of a Chemical Attack: A Systematic Approach to Rescue Operations*. Montgomery County: Maryland, 2001.

¹¹² City of Phoenix. Phoenix Regional Standard Operating Procedures. *Hazardous Materials Weapons of Mass Destruction Chemical, Biological, Radiological*. Phoenix: Arizona, 2000.

¹¹³ Montgomery County. Montgomery County, Maryland Fire and Rescue Service. *Managing the Consequences of a Chemical Attack: A Systematic Approach to Rescue Operations*. Montgomery County: Maryland, 2001.

¹¹⁴ City of Denver. *City and County of Denver Emergency Operations Plan*. Denver: Colorado, 2002.

¹¹⁵ Langtry, John. Assistant Divisional Officer. Northern Ireland Fire Brigade. Telephone Interview. July 16, 2003.

¹¹⁶ United Kingdom Home Office. *Strategic National Guidance. The Decontamination of People Exposed to Chemical, Biological, Radiological or Nuclear (CBRN) Substances or Material*. United Kingdom. February 2003.

the RDD site. It was constructed using the observations from data collectors at the incident site. All times are noted in Pacific Daylight Time (PDT) unless otherwise specified.

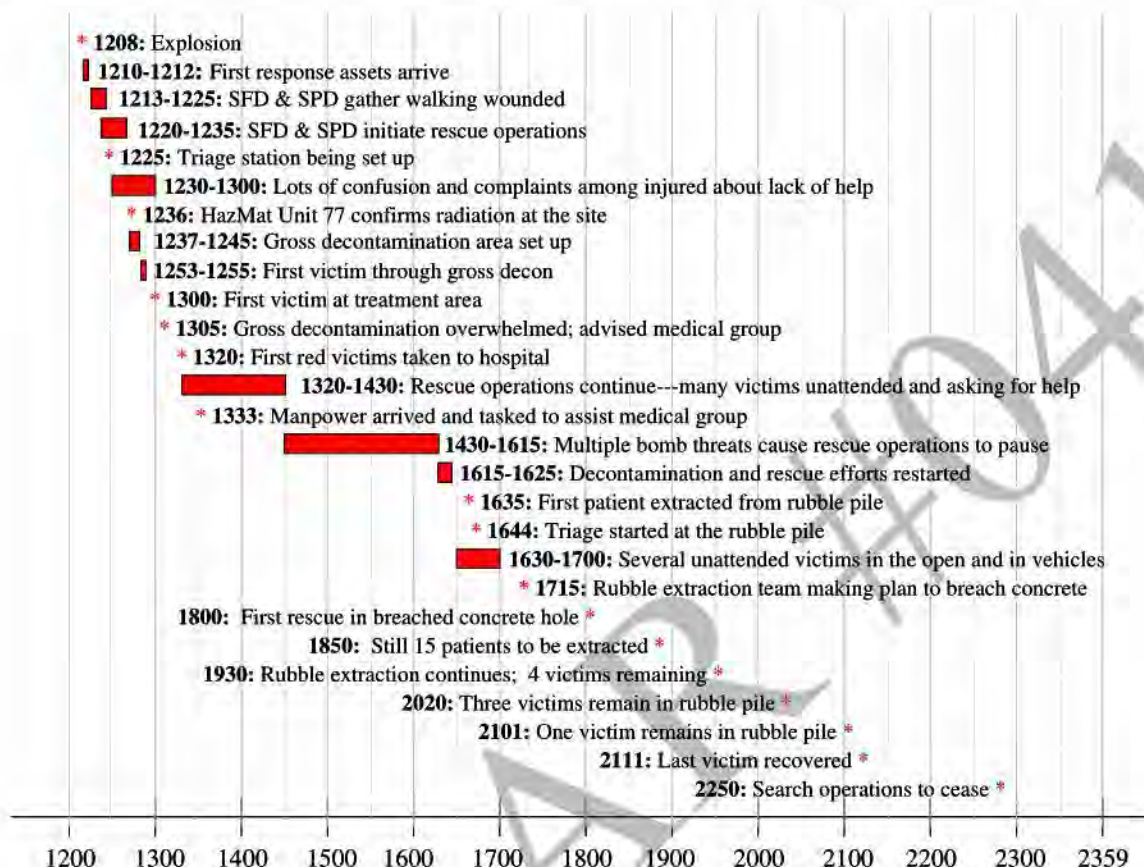


Figure 27. Reconstruction of Rescue Operations at the Radiological Dispersal Device Site

Incident site observations indicate that within minutes after the simulated RDD explosion on May 12, 2003, police cruisers, fire engines, and ambulances arrived at the scene. The responders, in particular Seattle Police Department (SPD) personnel, first gathered all walking wounded and removed them from the scene. SFD repeatedly made announcements over the loud speaker instructing anyone who could walk to slowly approach Engine #2 and that help was on the way. SPD was observed searching through the rubble and vehicles, administering first aid, and directing victims to Engine #2. SFD was also observed using ladders to get victims out of buildings. All of these events occurred within 14 minutes of the explosion.

Observations of the response took on a different tone after 1222¹¹⁷ when the first reports of radiation reached the incident site. HAZMAT arrived at 1227 and immediately started to take readings. There was much confusion at the incident site with several accounts of victims crying for help with no response from rescuers.

¹¹⁷ All times Pacific Daylight Time.

At the same time that HAZMAT was taking initial readings, SFD was also setting up triage, treatment, and decontamination stations. According to logs from data collectors observing the incident site, a triage station was being set up by 1225,¹¹⁸ a treatment station was set up by 1243, and a decontamination station was set up between 1237 and 1252. The first victim was moved through the decontamination station at 1253, and the first victim was observed at the treatment station at 1300.¹¹⁹ At 1305, the decontamination station reported that they were overwhelmed with victims. There was no indication that they got any assistance until 1333, when additional personnel arrived and were tasked to assist the medical group.

During a typical mass casualty incident, victims are tagged with colored tape or paper based upon the extent of their injuries. Victims with red tags have life threatening injuries and require immediate care. Victims with yellow tags need treatment but could sustain a short delay. Treatment of victims with green tags can be delayed until the more seriously injured victims have been cared for. Figure 28 shows the times that victims with red, yellow, and green tags were transported from the incident site to a hospital according to data obtained from hospital control. The first two red victims were taken at approximately 1315.¹²⁰ From 1315 to 1508, a steady stream of victims was taken to area hospitals. From 1315 to 1424, only the more serious red and yellow victims were transported, and then from 1424 to 1508 mostly green victims were taken to the hospital. This suggests that there was a lull in the response and no seriously injured victims were rescued and taken to the hospital. In fact, rescue operations had periodically been delayed due to reports of sniper sightings and potential secondary explosive devices prior to 1430 and were halted at approximately 1430 because a secondary explosive device was found at the incident site.

Rescue, treatment, and decontamination operations started again between 1615 and 1630, and as shown in figure 28, victim transport was restarted at 1638. Mostly red and yellow victims were taken to area hospitals between 1638 and 1814, at which time hospital control ended operations. The data show that prior to the pullback at 1430, a red or yellow victim was transported every 3.4 minutes; after rescue operations resumed the transport rate increased to one red or yellow victim transported every 1.6 minutes. It is not clear what led to an increase in rate of victims transported.

¹¹⁸ The evaluation team has no data indicating the level of activity at the triage station at this early stage of the response, and no data indicating when the triage station was operational.

¹¹⁹ The evaluation team has no data indicating the severity of injuries for the victims moving through the decontamination and treatment stations at this early stage of the response.

¹²⁰ Note that the data do not indicate if these patients were the first patients to go through decontamination or if the red patients went through decontamination at all.

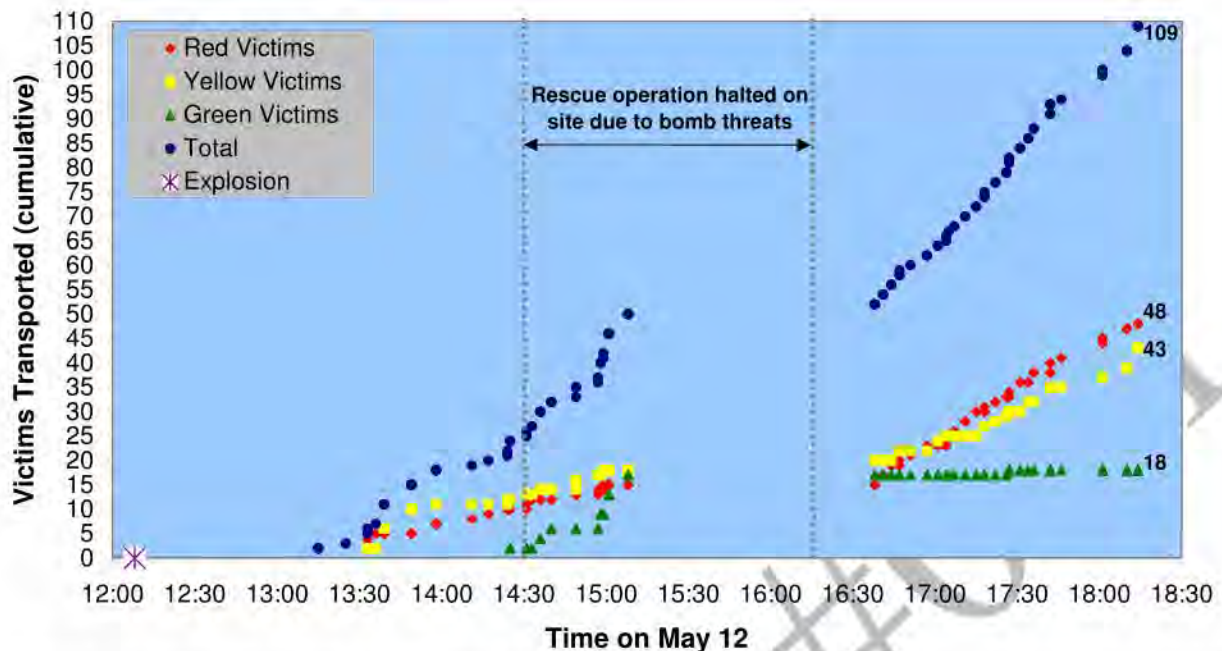


Figure 28. Transport of Victims from Incident Site¹²¹

According to data obtained from Harborview Hospital, which was hospital control during the exercise:

- A total of 109 victims were transported to area hospitals during the time that hospitals participated in the exercise: 48 red, 43 yellow, and 18 green victims; and
- At the beginning of the exercise, 150 volunteers were placed in the incident site. Therefore, 41 victims remained on the incident site when hospital play ended.

However, the log kept by hospital control differs with the tracking data kept by exercise control. According to exercise control:

- A total of 115 victims were transported to area hospitals: 34 red, 46 yellow, and 35 green;
- Responders rescued an additional 13 victims too late to be processed by the hospitals. These victims were still loaded into ambulances, but taken directly back to Union Station; and
- An additional 22 victims were not rescued until after hospital exercise play ended.

The evaluation team was unable to determine why there was a discrepancy in the two logs. Possible explanations include:

¹²¹ Data from Harborview Medical Center Mass Casualty Incident Patient Tracking Log and Seattle King County Public Health Incident Log.

- Exercise control assigned an injury status to each of the victims at the start of the exercise. Responders may have re-classified victim status during the course of the exercise;
- It is possible that there were additional victims transferred to area hospitals from 1511 to 1608 when hospital control was temporarily transferred to Overlake Hospital; and
- It is possible that the 13 victims recorded by exercise control that were processed and transported to Union Station after hospital control ceased operations were not recorded by hospital control.

4. Artificialities

During the FSE, a number of artificialities affected how players responded to the RDD incident, as well as some players' perceptions of the response and are, therefore, factored into the analysis. The artificialities included:

- Responders were at an advantage because they knew that the scenario involved an RDD explosion. Furthermore, many responders were aware of the concerns that came out of TOPOFF 2000 and other real world or exercise events—that responders went into an incident site so quickly they became casualties themselves. Therefore, during the FSE, many first responders did not rush into the scene when rescue operations began.
- Exercise control expected to have 200 moulaged victims for the exercise. Based upon initial planning for the exercise, hospitals expected ninety percent of all victims to be transported by 1800. This translates to 180 victims transported. However, there were 50 volunteer no-shows on the morning of May 12, 2003, so there were only 150 moulaged victims. Hospital control was not aware of this change. So they were expecting more patients than were available; this may have exacerbated medical and public health concerns about the overall rescue.

5. Analysis

Observations from the incident site from the first hour after the explosion indicate that after radiation was detected, responders were held back while HAZMAT teams conducted an initial assessment of the situation. While hospital control was aware that radiation had been detected at the incident site, there is no indication in the data collector logs that incident command or the medical group at the incident site communicated with hospital control to explain the need to conduct a more detailed risk-benefit analysis before rescue operations could commence.

After the first hour, the response became more typical—victims were pulled out of the incident area, assessed, and transported to the hospital based upon the severity of their injuries. However, rescue and decontamination operations were periodically halted and eventually ceased for almost two hours due to secondary bomb threats.¹²² This caused a similar delay in the transport of victims to area hospitals. There is no evidence in the data collector logs that indicated hospital control or the individual hospitals were aware of this delay. Similarly, there are no data from data collectors at the incident site indicating that the medical group or incident command

¹²² This delay would likely have been even longer if exercise control had not injected that the secondary explosive device was far enough away that it would not impact rescue operations.

communicated with hospital control about the discovery of a secondary explosive device. After the FSE, a hospital controller confirmed that the hospitals were unaware of the secondary explosive device.

6. Conclusion

Rescue operations at the RDD incident site during the FSE highlight the need for incident command and hospital control to communicate with each other during an emergency, especially one involving WMD. The public health and medical communities should be made aware of the need for incident command to conduct a detailed risk-benefit analysis prior to the start of rescue operations. These communities also need to be aware of the actions rescuers will take if a secondary explosive device is found and the impact that will have on victim rescue and transport. In addition, incident command must communicate with the public health and medical officials so that they understand the situation.

While it didn't occur during the FSE, it is extremely likely that in a real-world emergency the media would have become aware of the delay in transporting victims to hospitals. Without a concerted message from the public health and responder communities concerning the need to balance responder safety and victim rescue, a public outcry could have ensued. Therefore, public information personnel from both of these communities need to be educated about expected emergency response procedures during a mass casualty incident, especially one involving WMD. In addition, they also need to be kept informed by their respective leadership to ensure a consistent message is presented to the media and the public.

SUMMARY OF CONCLUSIONS— BALANCING THE SAFETY OF FIRST RESPONDERS AND THE RESCUE OF VICTIMS:
Operations at the RDD incident site highlighted the need for robust communications between hospital control and incident command.
The medical and public health communities need to be educated concerning the activities that first responders will take when faced with a potential terrorist incident involving WMD.
Public information personnel from the first responder, medical, and public health communities should also be educated about expected emergency response procedures so that the media and, therefore, the public are given one consistent message during an incident.

This page intentionally left blank

VI. ANALYSIS OF THE SIX CORE AREAS

1. Introduction

These six core areas of analysis were identified early in the Top Officials (TOPOFF) 2 (T2) planning phase by reviewing the TOPOFF 2000 After Action Report (AAR), lessons learned from 9/11 and the following anthrax attacks, Federal, State, and local participant objectives for T2, previous weapons of mass destruction (WMD) exercise AARs, and WMD training materials. Although the issues differed somewhat in content and presentation, they displayed considerable underlying similarity, and naturally clustered into six core areas of analysis. While these areas are closely interrelated, they are distinct. Viewing the exercise in light of these areas provides a useful organization of observations and ideas.

These areas of analysis include:

- Emergency public policy and decision-making;
- Emergency public information;
- Communications, coordination, and connectivity;
- Jurisdiction;
- Resource Allocation; and
- Anticipating the Enemy.

Because emergency public information played such a central role in each of the pre-Full-Scale Exercise seminars, as well as the Full-Scale Exercise (FSE), particular emphasis is placed upon this area.

2. Instances of challenges and good practices

In the various building-block seminars and the Large-Scale Game (LSG) leading up the FSE, several issues, or challenges, emerged that are relevant to the six core areas of analysis. In addition, a number of potential good practices were identified by seminar and LSG participants. During and subsequent to the FSE, the evaluation team identified instances of these challenges and good practices that occurred during the exercise. *Instances* are defined as occurrences that played out during the FSE. In several cases, challenges and good practices arose during the FSE that were not anticipated by the seminar and LSG participants. These were identified and catalogued by the analysts as well.

For each core area, a brief introduction and background are provided. This allows for an FSE-based context, such as key events and challenges that occurred within the areas, for discussions of the area. This is followed by a discussion of the key challenges and good practices in which feedback from the seminars and the LSG is examined and compared to the issues that arose during the FSE. Finally, conclusions are drawn and suggestions are made as to how these issues could be tested in future exercises.

This page intentionally left blank

A. Emergency Decision-Making and Public Policy

1. Introduction

Public policy and decision-making during an emergency differs from day-to-day policy and decision-making. The difference is even more significant during an emergency as a result of a terrorism attack. In such emergencies, top officials face especially difficult, political decisions under conditions of uncertainty characterized by unknown, or changing, information-baselines. For example, public health considerations might make quarantine a seemingly obvious choice. But, as was observed regarding Top Officials (TOPOFF) 2000 by Biodefense Quarterly in September 2000:

*Decisions regarding patient isolation, travel advisories, home curfews, the closure of airports and highways, and attempts to “quarantine” cities and states must be balanced against the practical feasibility of such measures, and their implications for civil liberties.*¹²³

This area examines the unique challenges, difficulties, and nuances of decision-making and policy-making in the initial aftermath of a terrorist weapons of mass destruction (WMD) attack.

2. Background

Despite foreknowledge of the scenario by some but not all, top officials and other decision-makers faced numerous challenging decisions throughout the course of the exercise. Some of these decisions are provided in Table 10.¹²⁴

¹²³ Inglesby, Thomas, Grossman, Rita, and O’Toole, Tara, “A Plague on Your City: Observations from TOPOFF,” *Biodefense Quarterly*, Volume 2, Number 2, September 2000.

¹²⁴ Decisions shown do not necessarily represent every decision made by top officials in these jurisdictions, but rather a sampling of the primary emergency public policy-related decisions.

Table 10. Examples of Emergency Public Policy Decisions Faced during T2

WASHINGTON VENUE	ILLINOIS VENUE	FEDERAL AGENCY/EXECUTIVE
<ul style="list-style-type: none"> • Determination of shelter-in-place order. • Issuance of mayoral and county proclamations of civil emergency. • Issuance of mayoral and county delegations of authority. • Issuance of governor proclamations of state of emergency. • Governor's request for Presidential Declaration of Major Disaster. • Implementation of exclusionary zone by city officials. • Closure/re-opening of road system by Washington Department of Transportation (WDOT) and city authorities. • Implementation of food control zone by state officials. • Determination of protective actions under condition Red by all affected jurisdictions. • Evacuation from shelter zone by city, county, and state officials. • Controlled re-entry to exclusion zone by emergency workers and members of public. • "Initial return" by state officials to allow people to return home in areas that did not appear to be affected by blast. • Radiological remediation and recovery criteria 	<ul style="list-style-type: none"> • Determination of protective action guidelines (PAG) for containing the plague (shelter-in-place) by state officials. • Issuance of mayoral and county proclamations of civil emergency. • Issuance of mayoral and county delegations of authority. • Issuance of governor proclamations of state of emergency. • Governor's request for Presidential Declaration of Major Disaster. • Closure/re-opening of the road system by Illinois Department of Transportation (IL DOT). • Executive Order #3 - suspended pharmacy practice act to let non-pharmacist to dispense prophylaxis and to do so outside of pharmacies. • Executive Order #4 - authorization to implement quarantine. • Determination of protective actions under condition Red by all affected jurisdictions. • Determine priorities for distribution of the Strategic National Stockpile (SNS) by Illinois State. • Re-opening of roads by IL DOT. • Medical decisions: <ul style="list-style-type: none"> —where to move critically ill, versus exposed, versus worried-well, versus other patients. —whether to convert specific rooms or an entire building to negative pressure, if the capability exists. —determination of how long patients should stay at hospitals. —determining how patients would get home when discharged under condition Red. 	<ul style="list-style-type: none"> • The elevation of the seven-city alert level to Red by the Department of Homeland Security (DHS) based upon the radiological dispersal device (RDD) attack and intelligence. • The elevation of the national alert level to Red by DHS based upon the RDD and bioterrorism attack. • Presidential Declarations of Major Disaster and Emergency in the states of Washington and Illinois, respectively. • Declaration of a Public Health Emergency by the Secretary of the Department of Health and Human Services. • Closure of airspace by DOT/Federal Aviation Administration (FAA). • Federal restrictions on food distribution by regional Federal Drug Administration. • Re-opening of airspace by FAA.

3. Discussion of challenges/good practices

In the seminars leading up to the Full-Scale Exercise (FSE), Top Officials (TOPOFF) 2 (T2) participants identified numerous challenges and some good practices related to *Emergency Decision-making and Public Policy*. Almost all of the challenges and good practices were observed during the FSE. This is additional evidence that foreknowledge of the scenario in an exercise does not necessarily result in foregone conclusions. While all the core areas of analysis in T2 are interrelated, the area with the greatest impact on emergency decision-making is that of

Communication, Coordination, and Connectivity. The ability of decision-makers to obtain or discern reliable, validated, timely, and understandable information to inform their decision-making emerged as a primary challenge throughout the exercise.

Table 11 depicts the challenges, and good practices relevant to *Emergency Decision-making and Public Policy* that arose in the seminars, as well as the instances that show how these issues played out during the FSE. Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A () is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or which the data indicate worked well;¹²⁵ these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and that had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require the continued attention of the national response community to facilitate smoother responses in the future.

¹²⁵ References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

Table 11. Emergency Decision-Making and Public Policy Issues during T2

ISSUES	SEMINARS/LSG					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	<i>Emergency Public Information</i>	<i>Radiological Dispersal Device</i>	<i>Bioterrorism</i>	<i>Direction & Control</i>	<i>Large-Scale Game Consequences</i>	
a. Understanding what decisions need to be made and by whom.		✓	✓	✓	✓	See "Jurisdiction" Core Area (+) Washington State Emergency Operations Center (EOC) attempted to use defined decision processes. (+) Seattle EOC representatives cross-fertilized decisions. (-) Some uncertainty in road re-opening authorities. (-) Some uncertainty in airspace re-opening authorities. (-) Some uncertainty in authorities to re-open facilities where plague was released.
b. Making decisions under conditions of uncertainty: accuracy versus timeliness of decisions.		✓	✓		✓	(+) Radiological dispersal device (RDD) site leaders recognized that decisions needed to be made without all information. () The shelter-in-place zone had to be expanded in Washington. () Discussion on size of exclusion zone. () Road openings in Washington would likely have had to be re-closed due to plume. () First responders in Washington held back on victim rescue pending preliminary risk-benefit analysis.
c. Handling international implications of decisions (transportation, security, etc.) and having consistency in decisions across borders.	✓			✓	✓	(+) Numerous instances of Department of Homeland Security (DHS) and other agencies interfacing with international authorities.
d. Making the notable, politically charged decisions (quarantines, Strategic National Stockpile (SNS) distribution, etc.) and how to handle them.				✓	✓	() Officials in Chicago suggested requiring proof of presence at one of the release sites to receive prophylaxis. () Quarantine was considered in Illinois. () Whether other countries could access the stockpile was considered.

ISSUES	SEMINARS/LSG					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	<i>Emergency Public Information</i>	<i>Radiological Dispersal Device</i>	<i>Bioterrorism</i>	<i>Direction & Control</i>	<i>Large-Scale Game Consequences</i>	
e. Management of economic impacts of increased security measures.				✓	✓	(+)Information Analysis and Infrastructure Protection Directorate in DHS examined economic impacts of nationwide alerts. (+) Agencies at all levels documented the projected economic impacts of security measures.
f. Understanding the extent to which the Threat Condition Red changes every aspect of decision-making.				✓		(-) Most agencies were uncertain what actions to take in response to an elevation of the Homeland Security Advisory System to Red.
g. Handling/understanding long-term restoration impacts.					✓	NA. Not played.

a. Understanding what decisions need to be made and by whom, and knowing who to have at the table

This issue is inherently related to the core area of *Jurisdiction* (See the “Jurisdiction” *Core Area*), but it has significant implications in the arena of emergency decision-making. Emergency policy decisions in the aftermath of a terrorist WMD attack are challenging enough, but not knowing who has the authority to make what decisions adds tremendously to the challenge. Such uncertainty not only impacts public relations (to the extent it increases the chances of inconsistent messages going out, or messages that may need to be altered later), but it also multiplies the inter-agency coordination burden as agencies feel their way through the process under the pressure of an unfolding disaster.

The *Jurisdiction* core area examines the jurisdictional uncertainties that participants experienced during the exercise, almost all of which arose in the context of decisions. Transportation emerged as a primary area where many were not aware of the various authorities for closing and re-opening elements of the nation’s transportation system, including roads, airspace, the rail system, and ports. Other issues where decision-making was unclear included Homeland Security Advisory System (HSAS) threat elevations (see the “Alerts and Alerting” *Special Topic*), and re-opening the facilities in Illinois where plague was released.

Another issue faced by decision-makers is not always having the right people involved in the decision-making process, and sometimes not knowing who the right people are. Both of these factors can make the unique challenges of this core area—making difficult policy decisions under conditions of uncertainty—more challenging. Likewise, improvements in the decision-making process can help reduce the uncertainty in some decisions, and increase the credibility of difficult decisions faced during such times. There were instances of the FSE during which decisions were not coordinated with all relevant parties. Perhaps the most dramatic example of this was when decision-makers at Federal, State, and local (FSL) levels were challenged to make policy decisions based upon the potential radiological contamination in the Seattle area. Setting aside the difficulties they experienced confirming the extent of the contamination (See the “Data Coordination” *Special Topic*), top officials needed experts who could translate detailed technical data into plain-language to aid them in the policy decisions they faced.

Not all agencies had the needed technical expertise on hand. In the words of a King County Emergency Operations Center (EOC) participant, “translating technical data on radiation into meaningful ‘so what’ terms and coordinating this was difficult. It took us three days to find someone [decision-makers] could understand.” The Washington State Department of Health acknowledged in the venue Hotwash:

Our biggest policy issue was around data—we were data rich and information poor. We did not have one place where highly technical data were being analyzed in one place. The result was that different policy rooms were making decisions based upon the data they had, which were probably right based upon the data they had, but not consistent with others.

Federal resources designed to assist decision-makers in translating technical data into meaningful terms were often not effectively utilized during the exercise. For example, the Advisory Team, which provides Protective Action recommendation support for decision-makers under the Federal Radiological Emergency Response Plan (FRERP), was not accessed by local decision-

makers. This struggle to understand the implications of detailed technical data, despite knowledge of the scenario by some, demonstrated that decision-makers were not assisted in this particular area by knowledge of the scenario.

The City of Chicago and the collar counties also noted in their Lessons Learned Reports from T2 the importance of having the right people in decision processes, stating that EOCs must be staffed with decision-makers, not just information gatherers. They also noted the importance of configuring seating arrangements in the EOC to have similar disciplines grouped together. One example of a good practice is that WA State EOC staff appeared to have defined decision processes that they used in their decision-making. Designed by the emergency managers who work there, the WA State EOC facility floor plan and building design promotes collaborative decision-making and information flow with its open floor structure, video teleconference capability, and electronic information sharing systems. In addition, a data collector in the Seattle EOC remarked that the EOC appeared to have substantial representation from various disciplines on hand to cross-fertilize decisions, and there appeared to be processes by which designated staff was empowered for emergency decision-making when the Mayor was absent.

b. Making decisions under conditions of uncertainty: accuracy versus timeliness of decisions.

The spokesperson for the City of Seattle at the venue Hotwash summarized this issue well when he said to the audience, reflecting on his experience from the FSE, “Nothing is static—the plume changes, evacuation zones change, etc. A solved problem is maybe only temporary—a final decision this hour may be a different decision the next hour.”

Top officials are routinely challenged in real life to make decisions under conditions of uncertainty. In both the Washington and Illinois, decision-makers were faced with the challenge of making decisions under conditions of imperfect information. In some cases, needed information was forthcoming in time (such as knowledge about whether an outbreak of Pneumonic Plague is naturally-occurring or an act of bioterrorism). In others, the information was unknown or may be based upon imperfect data, still requiring interpretation. In both cases, decision-makers must weigh the relative costs of time—the delay while waiting for the information base to improve—against the costs of less-than-perfect information.

T2 provided opportunities for decision-makers to explore these tradeoffs. The role of the Department of Homeland Security (DHS) is to assess the risk of terrorist attacks (a very imprecise task by definition), and to implement preventative measures designed to prevent or thwart attacks. This is an exceptionally difficult task replete with uncertainty. However, the Secretary of DHS cannot afford to wait for certainty to act—*certainty* for the Secretary of DHS is defined as an attack.

Perhaps the most dramatic decisions that were made during the FSE were those by the DHS Secretary to elevate the national alert system to Red first in seven select cities, and then nationwide (the City of Seattle and King County both elevated their jurisdictions to Red in the wake of the radiological dispersal device (RDD) blast—this is discussed in more detail in the “Alerts and Alerting” *Special Topic*). Of course in the exercise this was notional, and based upon notional intelligence. Likewise, in the exercise the real implications of a nationwide red alert could not be played. But the decision process and decision tradeoffs that the DHS Secretary and the Homeland Security Council (HSC) considered were real. And agencies’ responses, if

only to express great concern at the cost of maintaining a condition Red posture given a nonspecific threat, were also real. They challenged leaders to refine the HSAS system so that it achieves the intended goal of preventing future attacks in a way that, if possible, is more specific to localities at greater risk and minimizes unintended consequences.

In Washington, many policy decisions were made under conditions of uncertainty. The shelter-in-place parameters, the size of the exclusion zone, boundaries of the food zones, and road closures all depended on information regarding the size and nature of the radiological contamination. In anticipation that decision-makers would receive limited data in the early hours following the RDD incident, the Washington Department of Health, Public Health Seattle/King County, and the EPA developed default Protective Action Guidelines (PAGs) prior to the FSE. The Seattle Mayor implemented these *default* PAGs during the early hours of the incident, as decision-makers awaited the collection of the data required to effectively model the radiological contamination. During T2, as in reality, information changed over time, and some decisions had to be re-examined. Decision-makers in the WA venue, for example, expanded the shelter-in-place parameters once, and held heated discussions regarding the size of the exclusion zone. They also confronted the political issues of opening and then potentially having to re-close transportation systems based upon the recognition that they did not have all the information needed for these decisions. Operational decisions at the incident site were made in the midst of uncertainty, such as how long to wait for confirmation of radiation readings before rescuing victims, although it was somewhat influenced by artificiality. During T2, there is evidence to suggest responders held back from rescuing victims until a preliminary risk-benefit analysis could be done.

In the bioterrorism attack in Illinois, decision-makers were constantly challenged to make decisions under uncertainty. For reasons both of exercise artificiality as well as coordination challenges between agencies, tracking patient numbers was extremely difficult. Hospitals and the public health community were challenged to anticipate and plan for surge issues that would likely overwhelm the public health system within seven to ten days under the scenario.

And of course, throughout the exercise there was some uncertainty as to whether there would be additional follow-on attacks, though this was not aggressively played by most and was not specifically designed into the exercise.

c. Handling international implications of decisions (transportation, security, etc.) and having consistency in decisions across borders

The international scope of T2 was another ground-breaking element of T2 design. Represented through Canadian play and notional international injects, this expanded the scope of decisions and implications faced by top officials. On the domestic side, there were numerous instances of DHS and other agencies interfacing with international authorities in decisions such as transportation, food and import restrictions, border security, economic impacts of decisions, threat intelligence, and protective action measures. In the *National Direction and Control Seminar*, Canadian representatives stated that they would be interfacing with the Centers for Disease Control and Prevention on epidemiological data and tracking. They did just that during the T2 FSE. In addition, Canadian officials worked with DHS to place liaisons in Washington and Illinois. The DHS Office of International Affairs also coordinated extensively with Canadian counter-parts in all aspects of play to include the elevations of the threat condition to Red and addressing potential international economic implications of security measures and job

furloughs. Interestingly, in the seminar on bioterrorism, participants stated they did not think that cancellation of international flights would be likely once the plague epidemic spread internationally. This is another example of things not happening as expected during the FSE: the first cases of a mysterious illness were being reported from Vancouver as early as May 12, 2003. Within two days international (and domestic) flights were suspended as the U.S. transportation system was temporarily shutdown in Chicago. The Department of State (DOS) and Canadian AARs address international implications of the scenario and the lessons learned from the FSE in detail.

d. Making the difficult, politically charged decisions (quarantines, Strategic National Stockpile distribution, etc.)

During T2, decision-makers at all levels faced difficult decisions. The DHS decision to raise the red alert was surely a difficult one, and was discussed previously. In another example of a key decision, the Governor of Illinois requested a Presidential Declaration of Major Disaster to obtain federal assistance through the Stafford Act for the escalating bioterrorism disaster that had its epicenter in Chicago. This request was first denied, likely because it did not qualify under the language of the Stafford Act¹²⁶. In the end, this request was approved as an emergency declaration—and while purely notional, is nonetheless groundbreaking to the extent it challenged traditional interpretations of the Stafford Act.

Decision-makers in Illinois faced two difficult decisions: The potential need to implement a quarantine and how to distribute the limited initial supplies of the Strategic National Stockpile (SNS) before the arrival of the Vendor-Managed Inventory (VMI).¹²⁷ While officials never publicly used the term quarantine and did not notionally enforce it, the decision was made to close down air, sea, and rail transportation and to instruct the public to take a voluntary “snow day.” By May 14, 2003, the IL Governor had issued an Executive Order authorizing this and other emergency measures, such as releasing patient information to law enforcement and allowing licensed medical practitioners to operate outside of normal areas. Another Executive Order allowed non-pharmacists to dispense prophylaxis.

An interesting decision in Chicago was one where authorities required physical proof of exposure to one of the three known release sites as a prerequisite for receiving SNS medications, to ensure that only the initial exposed population (and its close contacts) received what were originally limited numbers of medication. This policy appeared to ignore the problem of secondary infections that the city and counties were beginning to deal with at that point, not to mention the possibility that other releases were still underway.

In an example of a good practice, city and state officials proactively acted to implement authorities to enable them to take extraordinary measures such as the ability to implement quarantine and to let non-pharmacists dispense prophylaxis and to do so outside of pharmacies should it be needed. DHS appeared to be researching legal authorities to implement a national quarantine should it be necessary.

¹²⁶ The Stafford Act was developed to address natural disasters or those with physical infrastructure damage.

¹²⁷ As described in the “SNS” Special Topic, it is an exercise artificiality that the push packages were deployed at all. In a real event, the SNS reaction to requests for SNS would have been to send the Vendor Managed Inventory, since Pneumonic Plague was already identified. Nevertheless, during the FSE top officials in Illinois had to make decisions as if they had a limited supply of prophylaxis.

e. Management of economic impacts of increased security measures.

The FSE did not play out long enough for players to have to manage the economic implications of increased security measures, with the exception of potential impacts relating to the various alert elevations to Red. There are numerous instances in which agencies at all levels actively considered such impacts. The Information Analysis and Infrastructure Protection Directorate within DHS examined economic impacts of the nationwide alerts on May 14, 2003. Concerns related to this were a dominant theme in the *Alerts and Alerting* session at the AAC.

These issues were front and center at the post-FSE tabletop exercise held in the Washington venue on May 15, 2003, and also at the LSG (see LSG AAR) held in December 2002¹²⁸. In the tabletop, participants recommended the involvement of the private sector to lend insights into this critical aspect of recovery and restoration. The Director for Economic Consequence Management at the Homeland Security Council was in attendance and stated that a Working Group would be established to initiate economic analysis using the Department of Commerce to evaluate the magnitude of the incident, and later develop two-week and two-month assessments to better understand the impacts. The Working Group would identify what federal resources might be available, but would work through local and State officials and the private sector to develop a local economic recovery plan and to make recommendations to the White House on needed resources.

During the LSG, participants in the economics group cited the need to conduct micro- and macro- economic disruption analysis; develop a long-term recovery plan; and catalogue available federal support across agencies. The Canadian delegation at the game predicted an increased focus on protecting national critical infrastructure and expectations that the private sector would start spending more on security, rather than waiting for government help. During T2, the private sector was minimally represented. Numerous participants suggested expansion of private sector participation in future TOPOFFs and the continuance of events such as the LSG to examine longer-term issues such as this.

f. Understanding the extent to which condition Red changes every aspect of decision-making

This issue was difficult to assess during T2, partially because many of the broad-reaching increased security measures one might expect under Threat Condition Red were already implemented (or in the process of being implemented) by the two participating venues as direct protective action responses to the specific attacks they were facing. Another reason this is difficult to assess is, as was discussed under the *Special Topic* section on alerts and alerting, there was widespread uncertainty on the part of most agencies as to what actions they should be taking in response to Threat Condition Red. This topic, for this reason alone if nothing else, merits continued attention and refinement by agencies at all levels. Future TOPOFF exercises might consider inviting States or cities that are not directly affected to participate in the FSE to gauge this and other national issues.

g. Handling/understanding long-term restoration impacts

Long-term restoration impacts were not played during T2 due to the duration of the exercise. They were addressed in the LSG where participants from FSL and international agencies, as well

¹²⁸ The LSG examined longer-term impacts in the aftermath of terrorist WMD attacks.

as the private and non-profit sectors spent three days actively discussing long-term restoration challenges in the aftermath of terrorist WMD attacks in three post-attack “moves:” Move I, 30 days out; Move II, 30 days through 6 months out; and Move III, 6 months out and beyond.

In Move II of the LSG, the issues centered primarily on the areas of decision-making and public information as participants cited ripple effects of security measures on the economy and international communities, the lack of a tax base to support needed revenue streams, continued issues in maintaining public confidence, managing economic impacts, managing calls for bureaucratic reorganizations, and managing growing accountability/liability issues with government actions. In Move III, participants were very cognizant of the fundamental shift in the national psyche that would have occurred by a campaign of terrorism attacks, and which would affect every sector, particularly the economic sector. They cited the tremendous drain on personnel and budgets in many localities, but specifically those directly affected by the RDD and bioterrorism attacks. They raised the issue of the continued and ever-present threat of future attacks, and how to improve prevention. Finally, they cited the numerous economic measures that would need to be taken by corporations and citizens to supplement the economy. Long-term remediation of a radiological incident site was not fully addressed during T2, not even during the LSG. In reality, it would receive heavy state, local, congressional, and media attention and would be one of the most critical aspects of response. The responsibility under existing plans for carrying out clean up activities is not clear under existing policies and should be examined in future exercises. Further the FSE did not play out long enough to fully exercise the public health implications of a bioterrorism attack. Participants unanimously cited the value of exercises that force them to confront and explore long-term restoration issues and impacts. The building-block structure of the TOPOFF Exercise Series lends itself to examining these issues.

4. Conclusions

Two groundbreaking decisions were addressed during the FSE that have not yet occurred in the real world:

- Elevations to red by City, County and Federal authorities (DHS); and
- Request for and issuance of a Presidential Declaration of Emergency for a bioterrorism disaster.

Decision-makers at all levels struggled with these and other difficult emergency public policy decisions, demonstrating that foreknowledge of the scenario by some participants in no way led to foregone conclusions.

The ability of decision-makers to obtain or discern reliable, validated, timely information, and to translate complex technical data into information that informs policy decisions, emerged as a primary challenge that underpins this entire core area. Quality decision-making does not mean that the decisions do not change or are permanent. Quality decisions are based upon the best information available at the time—information that sound processes help to ensure is valid. As the information-baseline evolves and decisions must be re-examined, there is a solid basis for the new decisions that emerge. Quality decision-making is marked by a thorough understanding and assessment of the tradeoffs at stake, which is only possible by having the correct expertise and decision authorities at the table.

The international scope of T2 and active participation of the Canadian Government expanded the scope of decisions faced by domestic top officials in the exercise. It represented a significant new element of the TOPOFF exercise design and participants have stated that it should be expanded upon in the future. The international implications of domestic decisions made during T2 are addressed with the T2 AARs produced by DOS and the Canadian Government.

While the economic impacts of terrorist attacks and resulting security measures and long-term restoration and recovery issues were not exercised during the FSE, participants throughout the exercise expressed continued interest in exploring these issues. Future TOPOFFs should expand on the concept of the LSG, which addressed long-term issues such as these in-depth. Finally, public response was not aggressively played during T2 and may be another element worthy of consideration to further challenge decision-makers in through branches and sequels in future exercises.

B. Emergency Public Information

1. Introduction

By definition, the term *emergency public information* reflects an understanding that public information during an emergency might differ from business-as-usual public information. Further, the task of those responsible for public affairs might vary according to the type of emergency—natural disaster or terrorist attack. For these reasons, those responsible for public information may find that despite the fact that they do their job every day, it becomes different, and very possibly more important, during a set of events like those that were simulated during T2.



The 9/11 attacks and the Maryland/Washington D.C./Virginia sniper attacks of 2002 demonstrated another unique aspect of terrorism regardless of scale: The acts may have been local in nature, but they were national in impact. These challenges caused emergency public information to emerge as a top issue in TOPOFF 2000 and in T2. T2 provided a context in which emergency public information strategies could be tested, examined, and refined under the challenge of dealing with two different, simultaneous attacks (with more potentially in motion).

The T2 design did not include an aggressive news-gathering function with multiple reporters calling the offices of top officials; it did not include substantial injects of simulated public responses to information; and it did not involve print or radio media outlets. Also, many of the most likely spokespeople in real emergencies—top officials—were not able to play at a level to truly simulate round-the-clock, real-world public information involvement. Special mention should be made though of those federal officials such as the Secretaries of DHS and HHS, as well as local officials such as the Mayor of the City of Seattle, who played extensively. However, these design elements, while potential considerations for future exercises, are not necessary to explore and exercise emergency public information issues. During T2, public information officers (PIOs) participated; media was simulated in some cases through the use of the Virtual News Network (VNN); and press releases were developed that, had this been a real-world event, would have been broadcast. This area of analysis examines those sources, as well as available broadcasts of real-time interviews by phone or in person through VNN, to understand what messages were (or would have been) delivered to the public, by whom and when.

2. Background

The first emergency public information challenges during the Full-Scale Exercise (FSE) arose in the wake of the unexplained explosion around noon on May 12, 2003, in the South of Downtown district of Seattle. The Mayor of Seattle, the Fire Chief, the Police Chief, and the Public Health Seattle/King County (PHSKC) Director held their first press conference 60 minutes after the explosion. The Mayor confirmed the presence of radiation in the explosion area and the PHSKC Director issued guidance to shelter-in-place in the central business district and other areas in the

vicinity. They instructed the public who may have been exposed to radiation to remove clothes, shower/bathe, lather, and not to consume food or water in the affected area.

Thirty minutes later a Seattle spokesperson announced the activation of the Seattle Emergency Operations Center (EOC). The public was urged to avoid areas within one mile of two cross streets in the affected area. Although it was not broadcast on VNN, Washington State released an announcement in this same timeframe noting the activation of the State EOC, outlining the State's role to monitor the situation, and reminding the public not to call 911 except for life-threatening emergencies.

The Department of Homeland Security (DHS) did not make a public statement about the explosion until nearly eight hours after the attack when DHS Secretary Ridge announced the elevation of the Homeland Security Advisory System Threat Condition to Red for seven cities. This may have been artificiality, but it is noteworthy.

In Illinois, public information challenges arose when the first patients began reporting to area hospitals with mysterious flu-like symptoms. The Mayor of Chicago addressed the city in the aftermath of the radiological dispersal device (RDD) explosion and instructed the city that the government was on higher alert. However, the bioterrorism attack had already occurred with releases in three locations on May 12, 2003. The Governor was the first to address the state and the nation regarding the outbreak of plague on May 13, 2003.

During the T2 building-block activities leading up to the FSE, but particularly in the seminar on emergency public information, participants identified numerous issues regarding public information. Many of these played out during the FSE. Examples include speaking with one voice, the need for more coordination on public health messages at all levels of government, finding the right contact in an organization, and the need for cross-border communications and coordination.

Participants in the building-block activities also cited concerns with public information related to the HSAS threat level. They mentioned the need to better understand what type of threat information to give to the public, the need to provide protective action guidance with threat levels, the need to balance threat fatigue with heightened anxiety, and the need to effectively handle the first hours of an attack before a Joint Information Center (JIC) can be established. Other concerns included managing rumors, the importance of clear and consistent messages from multiple spokespersons, the need to provide credible explanations for restrictive public policy decisions such as quarantines, and the need for accurate information to support decision-makers.

Table 12 depicts the challenges and good practices relevant to *Emergency Public Information* that arose in the seminars, as well as the instances that show how these issues played out during the FSE. Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A () is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;¹²⁹ these practices could potentially be explored further or promulgated on a broader scale. *Challenges*

¹²⁹ References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require the continued attention of the national response community to facilitate smoother responses in the future.

Table 12. Emergency Public Information Issues during T2

ISSUES	SEMINARS/LSG					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	<i>Emergency Public Information</i>	<i>Radiological Dispersal Device</i>	<i>Bioterrorism</i>	<i>Direction & Control</i>	<i>Large-Scale Game Consequences</i>	
a. Managing rumors, conflicts, and misinformation.	✓	✓	✓	✓	✓	(+) State and local agencies in Washington and Illinois contacted the Virtual News Network to dispel rumors. (+) City of Seattle appeared to give hourly press conferences.
b. “Speaking with one voice”—one message/multiple spokespersons.	✓	✓		✓	✓	(+) The Principle Federal Officials in Washington and Illinois emphasized the need for one message, and consistency with State and locals. (+) City/County/State joint press conferences were held in Illinois and Washington. (+) Regional Joint Information Center (JIC) in Washington and “joint” releases in Illinois. (-) Multiple phone numbers given for information in both venues. (-) Conflicting messages given by different officials and agencies. (-) Little coordination between Federal agencies and State/local JICs. (-) Inconsistent messages from City/County on safety of perimeter zone and food/water safety in Washington. (-) City/County and Federal messages had different themes about the radiological dispersal device. (+) Agencies in both Washington and Illinois used information provided by the Centers for Disease Control and Prevention’s (CDC) Health Alert Network (HAN) and other CDC sources.
c. Maintaining spokesperson credibility.	✓		✓	✓		Not exercised.

ISSUES	SEMINARS/LSG					FSE INSTANCES
	<i>Emergency Public Information</i>	<i>Radiological Dispersal Device</i>	<i>Bioterrorism</i>	<i>Direction & Control</i>	<i>Large-Scale Game Consequences</i>	GOOD PRACTICES AND CHALLENGES
d. Providing consistent Protective Action Guidance (PAG) for threat elevations and explanations of rationale for both PAGs and threat elevations.	✓	✓			✓	<p>(+) Rationale for shelter-in-place messages appeared to make sense, but later inconsistencies may have complicated things.</p> <p>(+) Rationale for “snow day”¹³⁰ guidance in Illinois made sense based upon disease transmission information.</p> <p>(+) Consistent messages in Washington regarding the shelter-in-place orders.</p> <p>(+) Chicago Mayor/Office Emergency Management explained protective actions for Red, and why more info could not be shared (security).</p> <p>(-) Very little guidance was given to the public in both national elevations to Red.</p> <p>(-) Little explanation for why entire country was elevated to Red.</p> <p>(-) Radiation guidance to public in WA was to shower, bag clothes, stay inside; but health workers were told to wear masks.</p> <p>(-) Plague guidance to public in Illinois was to stay inside and avoid those with symptoms, but health workers were told to wear masks.</p> <p>(-) Inconsistent treatment guidance for plague transmission: Illinois Department of Public Health (IDPH): Surgical masks; the CDC: Masks may not be necessary; the Department of Homeland Security (DHS): N-95 masks, goggles, glasses for healthcare workers.</p> <p>(-) Inconsistent messages on transmissibility of Pneumonic Plague (Ridge: “not contagious person to person”; CDC: “extremely transmissible,” CDC and IDPH: six feet; Canada: three feet.</p>
e. Handling early post-attack information when information is limited (pre-JIC).	✓		✓	✓		<p>(+) Top Officials at all levels appeared forthright about what wasn’t known.</p> <p>(-) Some statements were made prematurely and were changed later.</p>

¹³⁰ As used during T2, the phrase “snow-day” was to indicate that the public was to stay at home as if they were impacted by a major snow storm.

ISSUES	SEMINARS/LSG					FSE INSTANCES
	<i>Emergency Public Information</i>	<i>Radiological Dispersal Device</i>	<i>Bioterrorism</i>	<i>Direction & Control</i>	<i>Large-Scale Game Consequences</i>	GOOD PRACTICES AND CHALLENGES
						(-) Shelter-in-place zone had to be expanded.
f. Having pre-coordinated information packages.	✓			✓	✓	(-) Some agencies (e.g., CDC, City of Seattle) had pre-packaged material to disseminate or upload onto their website, but these packages were not coordinated with other agencies. <i>Agencies acknowledged in Hotwashes that this would have been helpful.</i> (+/-) Public Affairs staff in the Illinois State EOC Office of Human Services worked aggressively to anticipate questions the public would ask to coordinate answers. However, this coordination occurred after plague had broken out.
g. Ensuring accuracy.	✓			✓		() Attempts were made to ensure accuracy of information but coordination was extremely difficult. (+) Seattle/King County coordinated with City of Chicago for information sharing.
h. Coordinating cross-border messages.	✓			✓		Not played enough to assess.
i. Handling intense media pressure.				✓	✓	NA: Not played.
j. Balancing public information needs with national security needs.		✓				Not sufficiently played to assess.
k. Minimizing unintended consequences: (i.e., the worried-well).		✓				(-) Washington information was not sufficiently clear to avoid potential floods of worried well—especially since radiation is invisible. (+) Clear messages in Illinois on potential infected: At release site or person-to-person contact with symptomatic people. (-) Attempts to require proof of presence at release sites (Chicago/DuPage County).
l. NEW: Unclear language.						(-) Different technical terms used by spokespeople with no explanation. (-) Confirmation of diagnosis of non-specific “plague” by top officials. (-) Unclear distinction between essential/non-essential workers.

a. Managing rumors, conflicts, and misinformation

The artificiality of VNN, coupled with both the standard and large-scale information coordination issues experienced during any crisis, combined to create conditions where participants were able to exercise this challenge during T2 play. Rumors abounded during the FSE as they would in any real life crisis, and determining which rumors were true during the FSE proved no less challenging in many cases. For reasons that can be attributed to both the artificiality of VNN and information coordination issues, VNN carried information that was not always accurate. For example, on May 14, 2003, at 0945 Eastern Standard Time, the Department of Health and Human Services (HHS) was concerned that VNN was running numbers on plague casualties that were inconsistent with those given by their Secretary's Emergency Response Team (SERT). HHS public affairs contacted VNN to correct this. Coordination occurred between the State health department and Interagency JIC, and the City of Chicago held a press conference to attempt to correct this inconsistency. In the end, the explanation for the erroneous numbers was an artificiality: VNN stated that it was instructed to only report numbers that the Master Control Cell (MCC) gave them. But the exercise in rumor control was a valuable one. In Illinois, the Chicago Office of Emergency Management (OEM) contacted VNN to correct the address of one of the distribution sites that had been broadcast incorrectly.

In contrast, another rumor that was broadcast on VNN proved to be due to player actions—the rumor that Prussian Blue was being delivered at the request of the state. In fact, the state did not request Prussian Blue; the origin of this rumor was DHS, the Federal Drug Administration (FDA), and Federal agencies that were arranging for the delivery of this treatment through the Strategic National Stockpile (SNS). Participants at the Interagency JIC and the State EOC acted to dispel this rumor by contacting VNN, as well as Federal agencies in Washington, D.C.

The Washington State EOC called VNN to correct erroneous reporting that hospitals were overwhelmed. Seattle and King County attempted to dispel rumors on VNN regarding Marshal Law being considered (it was not). Finally, some organizations held hourly press conferences that would have been effective in helping to maintain a constant stream of “official” messages to the public. One agency, the Environmental Protection Agency, even had a rumor board to track down and validate rumors.

“Top Ten” Rumors in FSE Play*

1. There was a secondary explosion.
2. Air samples detected Strontium in the RDD.
3. **There are staff absences in Chicago hospitals.**
4. The Chicago airport is closed.
5. 18 Chicago hospitals are on virtual closure.
6. T2 exercise temporarily stopped in Chicago area on 5/14.
7. **Prussian blue was delivered to Seattle.**
8. The threat level was elevated for the nation at 1600 hours EDT on May 12.
9. Prussian blue is a protective paint.
10. **The RDD explosion occurred at noon on May 12.**

**Bolded rumors were true and others were false.*

b. Speaking with one voice—one message/multiple spokespersons

Not surprisingly, speaking with one voice proved to be one of the greatest emergency public information challenges experienced by participants. Table 13 depicts the many public information voices of various organizations over the course of the FSE.¹³¹

Table 13. Active Voices in Public Information during T2 FSE

ORGANIZATION	5/12/03	5/13/03	5/14/03	5/15/03
Washington Venue				
Washington State Emergency Operations Center (EOC)	■	■		
Seattle EOC	■	■		
Seattle-King County Regional Joint Information Center (JIC)	■	■		
King County JIC	■	■		
Washington Department of Public Health (DPH)	■			
Washington State Ferry	■			
Seattle Police	■			
Harborview Medical Center	■			
Federal Bureau of Investigation (FBI) JIC	■	■		
Federal/Interagency Venue				
Headquarters Department of Homeland Security (DHS)	■	■	■	■
DHS/Federal Emergency Management Agency (FEMA)			■	■
Headquarters Department of Health and Human Services (HHS)		■	■	■
HHS/Centers for Disease Control and Prevention (CDC)				■
HHS/Federal Drug Administration (FDA)		■	■	■

¹³¹ This table presents representative set of organizations that prepared or delivered messages for the public based upon press releases submitted at the close of the FSE and the VNN interview record. It does not necessarily reflect all organizations preparing such messages nor necessarily account for every day the depicted organizations were preparing such messages.

ORGANIZATION	5/12/03	5/13/03	5/14/03	5/15/03
FBI				■
Department of State			■	
FDA		■		
Department of Labor/ Occupational Safety and Health Administration			■	
State of Illinois Venue				
DHS-Chicago			■	■
FBI-Chicago				■
Office of the Governor		■	■	■
Illinois Emergency Management Agency		■		■
Illinois Department of Public Health			■	■
Illinois State Police			■	■
Regional JIC		■	■	■
City of Chicago/Office of Emergency Management	■	■	■	
Chicago Department of Public Health			■	■
Cook County Department of Public Health			■	
Kane County Department of Public Health			■	
DuPage County Department of Public Health	■	■	■	■
Lake County Department of Public Health			■	

While both venues implemented regional JIC concepts, the organizations shown in the table produced at least one independent press release. As many participants pointed out in the seminars, multiple spokespersons are to be expected in an event of the magnitude any weapons of mass destruction (WMD) attack would produce, and that is not necessarily problematic. In an emergency of the scale and psychological impact of a terrorist WMD attack, it is critical that government spokespeople speak with one voice and have a consistent message. But having one government voice is usually easier said than done and is an issue of coordination as much, or more, than one of politics.

During T2 there were instances of good coordination between Federal, State, and local government organizations in both the radiological and bioterrorism public information campaigns. In Washington, leaders were consistent with the public guidance to shelter-in-place following the radiological attack. They were generally consistent with protective action guidance to remove and bag clothes, take a warm shower, lather, and remain indoors. Jurisdictions were consistent with messages regarding transportation closures. In Illinois, leaders were consistent with messages telling people to seek emergency medical care immediately if they believed they were exposed to plague or were symptomatic. The leaders in Illinois were also consistent with transportation closure messages. Leaders at all levels attempted to reassure the public that the communities would get through this difficult and frightening time, and to remain calm.

There are numerous instances of organizations coordinating within and between JICs and reaching out from local to State to Federal levels. In both venues, the Principle Federal Official (PFO) from DHS emphasized and worked for a consistent federal message that was consistent with the State and local messages. In some cases, joint press conferences were held with representatives from the Washington State, the City of Seattle, King County, the JIC, and others.

However, there were a number of occasions where different voices were providing different messages—a fact that likely would have caused confusion. Tables 14 and 15 highlight messages that were conveyed via press releases from various organizations in Washington and Illinois. The messages were in five areas: relative danger, where to obtain information, protective action guidance, guidance regarding the red threat condition, and how to know if you were contaminated.

In Washington, the public was given five different phone numbers and at least two websites at various times for information relating to the RDD attack by organizations including the American Red Cross, the City of Seattle, Federal Emergency Management Agency (FEMA), King County, and Washington State. While each number may have served a distinct purpose, it was difficult to know for sure what number to call for what purpose, and they were not released as a coordinated “joint” set.

Finally, the Regional Disaster Plan signed by numerous agencies in the City of Seattle and King County designates the City of Seattle as the lead agency for a regional JIC. The City established a JIC at its EOC to which King County sent a representative. King County however, also established at least one JIC and proceeded to release messages independent of the City of Seattle that were not always coordinated. This contributed to inconsistent messages to the public.

Table 14. Public Messages in the State of Washington

Message Categories	Regional JIC	City of Seattle	King County IC	WA State	FBI JIC	FEMA	DHS	CDC ¹³²	FDA	American Red Cross
Relative Danger¹³³	Low	Medium	Low	Medium	NA	NA	High	NA	NA	
Where to get information	General Information: 866-4CRISIS	General Information: General Information: 800-555-HELP	General Information: 866-4CRISIS Crisis Clinic: 206-461-3200 King County Employees: 206-205-8600 Road Conditions: 206-296-8100 800-695-ROAD Schools: http://www.schoolreport.org www.govlink.org Sound Transit: 888-889-6368 www.soundtransit.org Water Taxi Information: (206) 553-3000 888-808-7977		877-940-4700 (tips)	www.fema.gov	NA	NA	NA	866-GET-INFO 206-323-2345 www.redcross.org
Protective Action Guidance	Shelter-in-place Shower Bag clothes Don't consume food/ water	Shelter-in-place Shower Bag clothes Don't consume food/ water	Shelter-in-place Shower Bag clothes Don't consume food/water	Shelter-in-place Shower Bag clothes Don't consume food/ water	NA	NA	NA	Prussian Blue	Prussian Blue	866-GET-INFO www.redcross.org
Guidance on Condition Red							Avoid public gatherings Don't go to school/ church.			866-GET-INFO www.redcross.org
How to know if you might be contaminated	You'd be sheltering.	You'd be sheltering.	You'd be sheltering.	You'd be sheltering.						

¹³² The Centers for Disease Control and Prevention (CDC) provided notional support to the states via its Health Alert Network (HAN) and their website. HAN messages do not go directly to the public; rather they are provided to State and local health departments, other government agencies, and medical organizations to support public information by those agencies. The T2 analysts did not have data from CDC's website.

¹³³ "Relative danger" refers to the relative overall danger of the RDD explosion that was conveyed to the public through various agencies/organizations.

The PHSKC Director stated at 1715 Pacific Daylight Time (PDT) on May 12, 2003, in a press conference that there are “little to no long-term health risks from this type of bomb” and that this was “not a health emergency.” Twenty minutes earlier, however, a Washington State Department of Health (DOH) spokesperson stated in a VNN interview that it was “too soon to tell” if there is danger in the downtown area. The type of bomb was not known yet (he had previously stated that officials were still trying to determine exact “radiological isotopes”) so the risks were still unknown. In another example, citizens were at first advised that the water was not safe and to only consume water in closed containers. Later that day, the Mayor declared the water system was safe. But more messages followed from the PHSKC, again instructing the public to only drink water in closed containers and to not let pets drink water from outside. Concerns regarding runoff of contaminated water were raised by health and environmental agencies, concerns which were later determined not be an issue.

In addition, Federal agencies such as the FDA appeared to be releasing messages regarding Prussian Blue, a radiation treatment for Cesium exposure, that were not coordinated with the State and locals officials in Washington. At 1800 PDT on May 12, 2003, the DHS Secretary announced on VNN that Department of Energy (DOE) would be delivering unspecified medications from national stockpiles. Federal agencies began coordinating the deployment of Prussian Blue by around 1300 PDT on May 12, 2003. While its deployment may be automatic with DOE as a resource for first responders, neither the local responders nor the State expected to need it or use it for the general public. To that extent, public announcements regarding it were not synchronized with other messages coming in from State and locals regarding the severity of the radiation contamination. The Washington State EOC and the Interagency JIC expressed frustration about DHS “making local announcements.”

During the first six hours of the RDD in Seattle, messages from the City, County, State, and Federal spokespeople effectively carried different themes. The city’s messages conveyed a disaster of a serious enough scale that a number of emergency public policies had been implemented, yet they conveyed the idea that sheltering-in-place was sufficient protection. The county’s messages attempted to reassure the public that there was nothing to worry about and that there were little to no long-term health risks. Finally, DHS Secretary Ridge reported on VNN, six hours into the disaster, that “we’re sending the National Stockpile” conveying a potential disaster of a sufficiently large scale that local resources were already overwhelmed.

In Illinois, messages appeared to be closely coordinated between State and local governments. The collar counties and the City of Chicago produced regular joint releases. Independently produced press releases by jurisdictions were rare. Overall, this resulted in consistent messages regarding instructions to the public and key themes: seek immediate treatment if symptomatic, remain calm, and Pneumonic Plague is contagious and serious but highly treatable. They released a set of information numbers for the public to use, with one number for each jurisdiction. However, there were some inconsistencies among jurisdictions regarding which antibiotics would be effective. The City of Chicago stated that Doxycycline was the treatment being used, Illinois mentioned the same medication and Ciprofloxacin, and the Centers for Disease Control and Prevention (CDC) mentioned four other antibiotics but not Ciprofloxacin or Doxycycline. The dominant guidance to the public, however, was to seek emergency treatment immediately if individuals believed they were exposed, so these inconsistencies might not have had dramatic effects.

Table 15. Public Messages in the State of Illinois

Message Categories	City of Chicago	State of IL (IDPH)	"Joint" City/County	Cook County	DuPage County	Kane County	Lake County	FBI	FEMA	American Red Cross	CDC
Prognosis	Deadly but treatable with antibiotics							NA	NA	NA	Deadly but treatable with antibiotics
Where to get information	312-743-INFO Animal Health: 217-782-4944	www.State.il.us/idph-dr/topoff_2 866-TOPOFF2		888-555-CURE	630-682-7000	800-555-6337	847-377-8130	877-940-4700 (tips)	800-621-FEMA	866-GET-INFO www.redcross.org	
Protective Action Guidance	<u>Antibiotics: Doxycycline</u> Cover mouth when cough/sneeze <u>Who should get Antibiotics:</u> (5/14) Only those exposed to release site (proof required) (5/15) Exposed to site or close contact with those directly exposed to site	<u>Antibiotics: Doxycycline /Cipro</u> <u>Who should get Antibiotics:</u> (5/13) Exposed to symptomatic persons. (5/14) Exposed to site or to symptomatic person.	<u>Who should get Antibiotics:</u> (5/14) Only those with symptoms should seek medical treatment, otherwise monitor condition. (5/15) Exposed to site or to symptomatic person	See "Joint."	(5/12) <u>Who should get Antibiotics:</u> Exposed to site or to symptomatic person	(5/14) <u>Who should get Antibiotics:</u> Exposed to site or to symptomatic person	See "Joint."	NA	NA	NA	<u>Antibiotics:</u> <i>Streptomycin</i> <i>Gentamicin</i> <i>Tetracycline</i> <i>Fluoro-quinolone</i> Disposable surgical masks
Guidance on Condition Red	Stay indoors.						NA		NA	NA	866-GET-INFO www.redcross.org
How to know if you might be contaminated	Exposure to one of release sites: (Terminal 3; later 2; later Int'l, which is terminal 5) 6 feet of symptomatic	Exposure to one of release sites: (Terminal 3; later 2; later Int'l, which is terminal 5) 6 feet of symptomatic					Exposure to Int'l terminal				Exposure to release site/6 feet of symptomatic

Also, there is some evidence of inconsistent guidance to the public as to who should seek antibiotic treatment, as there were up to four different messages given to the public:

- Only those directly exposed to the release sites or to symptomatic persons should seek antibiotic treatment;
- Only those who are symptomatic should seek antibiotic treatment;
- Only those who were directly exposed to release sites, or in close contact with those who were; and
- Pre-exposed persons considered at high-risk should seek antibiotic treatment (only one organization referenced this).

There was further inconsistency in messages citing the release sites relative to O'Hare International Airport. Some organizations cited the affected Terminal as Terminal 2, later changing it to Terminal 3 and later calling it the International Terminal (which is Terminal 5). At least one organization referred to the International Terminal as Terminal 3. At one point controllers advised at least one organization to use Terminal 2. There was also inconsistency in the guidance as to what information people should bring with them to the SNS dispensing sites. Only the City of Chicago and DuPage County appeared to publish such guidance, advising people to come prepared with personal and family identification, and information on drug allergies, pregnancy status, and use of contraceptive (City of Chicago only), weight and age of children, whether women are breastfeeding (City of Chicago only), and current medications and general health status (DuPage County only). One would expect to see this comprehensive checklist widely and consistently disseminated.

One message that did not appear to come out strongly or consistently was that of the potential need for surgical masks. Medical community communications reflect the critical importance of N-95 masks¹³⁴ in reducing the transmission of plague, even specifying that other commercially available masks would not be effective. However, masks were rarely mentioned in the press releases, and the specific N-95 mask was not mentioned at all. Medical communications also reflected concern that there might be a shortage of this type of mask due to the recent Severe Acute Respiratory Syndrome (SARS) outbreak, but this did not appear to be addressed in the media. In DuPage County, the EOC eventually arranged for a large order of N-95 masks for county hospitals.

The PFOs in both venues observed the lack of Federal agency coordination of messages with State and local governments when they arrived, and acted to improve this. The PFO in Washington noted concern about "unilateral messages from D.C." and that no messages had come to the JIC despite critical decisions such as the seven-city elevation to Red, road/airport closures, and the restriction of border crossings from U.S. Customs. The exercise did not play out long enough in either venue to see how the PFO affect this information flow, but the PFO role has the potential to strengthen and streamline the flow of key information between the State and local governments and Federal agencies during a disaster.

¹³⁴ N-95 masks are fitted surgical masks that provide protection against particulate inhalation of contagious biological agents.

c. Maintaining spokesperson credibility

Mr. Frank Sesno, former Washington Bureau Chief for CNN, alerted participants during the *Direction and Control Seminar* to be aware that the media will “follow you down your own dead ends” and report it. Fortunately, participants did not have to contend with this reality during FSE play since there was no active mock-media. For this reason, there was not sufficient data for this area to be addressed.

d. Providing consistent Protective Action Guidance and threat elevation guidance

Determining how much information to release regarding the rationale for threat elevations is a particularly challenging for decision-makers. Balancing the public’s need to know and understand certain information to ensure the overall protective posture is indeed elevated, can risk compromising national security. At the After Action Conference, participants voiced strong concerns regarding the lack of specific intelligence from official Federal to State and local channels regarding the nature of the threats or the rationale for threat elevations. In many cases specific information may not be known, but sufficient general intelligence exists to merit an increase in the nation’s threat posture. In other cases, classification requirements limit information that can be transmitted from the intelligence community to State and local governments. DHS is currently examining this issue.

During T2, little public information was given to explain the rationale for the threat elevations to Red. In fact, public announcements regarding the threat elevations were fairly confusing (See the “Alerts and Alerting” *Special Topic*), often leaving even government officials uncertain about the alert status of their jurisdictions.

The rationale for the regional Seattle-King County elevation to Red was probably self-evident because terrorism was formally suspected by the time of the announcement. In the seven-city elevation, DHS Secretary Ridge explained the decision as an action to take additional preventative action, based upon both the RDD attack and intelligence that suggested the listed cities may be at extreme risk. On May 13, 2003, when the DHS Secretary elevated the nation to Red, it was in response to the mounting cases of plague in Illinois and Canada. The public was advised to avoid public gathering places, such as churches, schools, and work for 48 hours. However, there was no mention as to why people in Topeka, Kansas, were at as great of a risk of attack as those in perceived high-risk areas such as Chicago or New York City.

In examining the Protective Action Guidance (PAG) messages that were prepared for public release, one issue that emerged was that the recommendations provided to the public were not comprehensive. Just after 1300 PDT on May 12, 2003, in a joint news conference held by the City of Seattle and King County, the public was advised that food and water in the area or that “may have been exposed” should not be consumed. No guidance was given at that time as to what food or water sources may have been exposed or how the public could tell. Later it was clarified that food or water in sealed containers, or food that was indoors, was safe to consume. A news release from the City of Seattle at 1330 PDT on May 12, 2003, advised that “most people” will not experience long-term health effects, but it also advised people to “not take in additional radiation.” It did not clarify who might be at risk for such effects or what it meant to “take in radiation,” which could appear to imply ingestion or inhalation. It advised people to follow the directions of officials who might decide to evacuate people from the immediate area, arrange medical treatment for those injured by the blast, and decontaminate those who were

contaminated, but it did not specify how one would know if they were contaminated. In fact, other messages stated that exposed people (even at the site) would not necessarily feel sick and noted that radiation cannot be seen. This could have led to an increase in the numbers of worried well and undermined the credibility of the spokespeople trying to reassure the public.

The news that evacuations were potentially being considered could have been problematic at a time when people were also being advised to shelter-in-place without the additional clarification that evacuations were intended as a safe and structured means to move those sheltering-in-place. Also, initial messages instructed the public not to call 911 except to report life-threatening emergencies; however, an alternate number was not offered until almost 90 minutes after the blast. Similarly, the public was instructed at first to shelter-in-place, take a warm shower, and bag potentially contaminated clothes. Ninety minutes after the first message, they were instructed to close windows and turn off ventilation systems, and bring pets inside and bathe them.

In Illinois, people were advised that Pneumonic Plague was potentially highly contagious through the inhalation of respiratory droplets. People could contract the illness if they were in close contact, which was defined as within six feet of an infected and symptomatic person. They were advised to stay home if possible, though essential workers were instructed to report to work. But only one jurisdiction specifically advised people to cover mouths when coughing/sneezing, and, during the first day of play, no jurisdictions mentioned wearing masks as an additional protective action measure. When the additional protective measure to wear masks was mentioned the next day, the commercial surgical masks were recommended, though health community e-mails indicated that only the N-95 masks were considered effective.

e. Handling early post-attack information when information is limited (pre-Joint Information Center)

In any disaster, particularly one involving a possible terrorist WMD attack, there is much that is unknown in the early hours after the incident, including:

- Whether the event is indeed a terrorist attack;
- Whether there will be other attacks; and
- The extent of the damage—particularly from radiological weapons or bioterrorism.

In the seminars, participants emphasized the importance of early and visible leadership from top officials. In Washington, the Mayor of Seattle was on the news within 60 minutes of blast. He confirmed radiation early on and issued shelter-in-place guidance to those in potentially contaminated areas. Those outside the defined area were told that they did not need to shelter-in-place. A combination of factors, such as confusion among agencies in determining the range and types of radiation (see the “Data Coordination” *Special Topic*), as well as changing environmental factors, changed the parameters of the contaminated area over time. This caused decision-makers in the Washington venue to enlarge the shelter-in-place and exclusionary zones.

In Illinois, the Mayor of Chicago addressed the city after the threat condition was raised to Red (the address was pre-taped), and the Governor addressed the State the same day that the epidemic of plague became evident. However, some key messages were delivered much later. For example, the news that plague can be transmitted through symptomatic people was given 24 hours after the first announcement. The public was not advised until May 15, 2003, about the

transmissibility of Pneumonic Plague through cats and about prophylaxis options. Also, immediate guidance was given instructing people to seek medical treatment if symptomatic, but specific antibiotic options were not formally mentioned.

f. Having pre-coordinated information packages

The suggestion for pre-coordinated, agent-specific information packages was made numerous times in the various seminars and the game preceding the FSE. While some agencies appeared to have some fact sheets, neither Illinois nor Washington appeared to have a robust set of pre-coordinated, agent-specific, off-the-shelf information packages. The City of Seattle did direct the public to its website (www.seattle.gov), where it later clarified that fact sheets on dirty bombs, radiation, self-care in times of crisis, and disaster planning and personal preparedness were made available; no public official or press release ever referenced these fact sheets or the availability of fact sheets in general. Public Affairs staff in the Illinois State EOC Office of Human Services worked aggressively to anticipate questions the public would ask and to coordinate a set of answers. However, this coordination occurred after the plague had broken out. The City of Chicago did produce a fact sheet on Pneumonic Plague that was sent out. Some Federal agencies, such as the CDC and the FDA, do maintain fact sheets but it was not clear which State or local agencies utilized them.

g. Ensuring accuracy

Ensuring complete accuracy of information in the midst of a crisis is extremely difficult. Decision-makers are constantly challenged to make decisions based upon imperfect information, and information that is changing (See the “Emergency Public Policy and Decision-making” *Core Area*). This is partly due to the rate at which a crisis unfolds, specifically those involving terrorist WMD, and partly due to issues with coordination and communication (See the Communications, Coordination, and Connectivity *Core Area*). However, as participants pointed out in the seminars, the importance of having as accurate an information-baseline as possible in an unfolding event cannot be understated.

During T2 there were challenges in maintaining accuracy of information. An example is the casualty counts at the RDD scene in WA. Casualty counts were mounting; yet a King County Public Information Officer, speaking for the regional JIC repeated twice in a May 12, 2003, press conference at 1600 PDT that there were “no casualties.” By this time there were more than sixty casualties and two deaths were reported in the EOCs. In Illinois, this challenge was equally difficult, as the size of the plague epidemic was growing daily. Leaders in Illinois had a very difficult time confirming accurate information regarding patient counts and fatalities (See the “Hospital Play” *Special Topics*).

Confirming patient numbers in the unfolding bioterrorism event in Illinois proved to be a tremendous challenge for a number of reasons, not the least of which was the artificiality of VNN having been instructed to use pre-scripted numbers from the MCC, which conflicted with the numbers being confirmed by players in the Chicago OEM. While this was an artificiality, the resulting challenge for players was probably emblematic of what happens in the real world with the media and its influence on perceptions of reality.

Ensuring accurate information depends upon having structured, well-defined and robust information flow strategies, where information is accepted from pre-defined validated sources. Such strategies exist in numerous policies such as the Interim Federal Response Plan, but

implementation of them remains a challenge. Regional JIC concepts are a critical element of such a strategy. Twenty-first century communications technologies both enable and challenge these strategies as they eliminate limits of time, distance, and hierarchical structures.

h. Coordinating cross-border messages

There was not sufficient data on the U.S. side to analyze this issue.

i. Handling intense media pressure

Because news-gathering and public reaction were not played during the T2 FSE, this issue could not be analyzed.

j. Balancing public information needs with national security requirements

This issue was not played in enough sufficient detail to be analyzed.

k. Balancing public information needs with national security needs

Because the intelligence process was notionally played during the T2 FSE, this issue could not be analyzed.

l. Minimizing unintended consequences

Minimizing unintended consequences is challenging by definition. Thorough coordination and clear, comprehensive, and consistent messages certainly help in this area. Because public reactions were not heavily played during the FSE, this area is difficult to assess based upon empirical data. However, there are some instances worth examining as they could have potentially resulted in unintended consequences.

On May 14, 2003, the Chicago DPH issued a press release announcing its distribution plan for antibiotics. It stated that proof of presence at one of the three suspected release sites would be required as a condition for receiving prophylaxis to prevent the lines from being too long. This seemed strange under the circumstances where a) theoretically other unknown releases could have occurred or could have still been occurring at that time—the nation was under Threat Condition Red; b) the majority of the infected victims by then were second generation cases who were in contact with people at the initial release sites. While this message was not formally retracted in the exercise, all jurisdictions in the Illinois venue had agreed by May 15, 2003, that anyone who showed up for treatment would not be turned away.

In both the RDD attack and the bioterrorism attack, managing the worried-well could have been a huge challenge for the public health and medical communities and public information officers. Clear and consistent guidance from credible spokespersons would be key to minimizing issues of the worried-well. Also, in the State of Washington, the exercise ended before officials were able to say with certainty what the potential long-term implications of any, or specific, radiation exposure might have been, thus limiting the ability to analyze this issue. But, little-to-no guidelines were offered to help people who believed they may have been exposed to radiation determine with assurance that they had not been exposed. This could have resulted in a flood of people to medical centers wanting to confirm whether they were contaminated.

m. Unclear language (new)

Language is critical in a time of crisis. Simple messages are especially important when seeking to maintain calm and invoke specific responses from the public. During T2, the use of technical language with little-to-no explanation proved to be a potential challenge for the audience. In Washington, terms such as *multiple alarm response*, *instrumentation to protect citizens*, *habitability check*, *external hazard*, and *not a health emergency* were used by various State and local spokespeople on the first day.

In contrast, the greatest language challenge for officials in the bioterrorism attack was one of being too vague. The IL Governor's initial speech confirmed the diagnosis of the mysterious respiratory illness as plague. The DHS Secretary, in his speech to the nation on VNN on May 13, 2003, opened by confirming that the mysterious illness in Illinois was plague, but did not specify the type of plague. Some Americans might have assumed he was referring to Bubonic Plague—the “Black Death” of the Middle Ages. In fact the participants at the Large-Scale Game assumed just that when the type of plague was not specified.

3. Conclusions

Emergency Public Information was a dominant theme in TOPOFF 2000 and emerged as a dominant issue during T2. It merited its own seminar, and participants raised concerns and identified issues in this area in every other seminar. It is not surprising that it emerged as an issue during the T2 FSE—unlike everyday public information, leaders in the midst of a disaster, especially one involving WMDs, are thrown into an environment of chaos where time and certainty compete, and the public's attention and demand for information are high. Often the public's safety is dependent on the effective communication and receipt of emergency messages. This produces an environment of great pressure on top officials to speak to the public and to release information—this may result in releasing information that could change, that has not necessarily been thoroughly coordinated, and that may not be consistent with other messages being released at the same time. The messages given to the public by officials are competing with a flood of non-official messages as well. Establishing consistent messages across all official spokespersons is key to maintaining credibility of official spokespeople and is one of the most effective ways to retain the public's attention regarding messages that may be critical to their safety.

Participants stated that the VNN element of the TOPOFF exercises was extremely valuable in simulating the realism of the media element. They have also said that they would like to continue to be challenged in the area of emergency public information through elements such as a robust news-gathering function and simulated public reactions. Many assumed that VNN was playing these functions during T2 when in fact it was not contracted to do so. It was intended primarily to lend an environment of realism to T2—not substitute for information sources. Interestingly, however, it is a parallel to the real world in which participants have acknowledged that they often rely on network news for information because formal channels are slow or nonexistent. The reconstruction of T2 illustrates the information validation issues that are multiplied when any media outlet substitutes for official channels of information.

The dominant issue that emerged from this area in the seminars and during the FSE remains one of coordination. Creating mechanisms that can support this coordination, in the midst of the chaos, is imperative. Ensuring accuracy of information is extremely difficult, and the

information will change. A consistent and comprehensive message that is based upon the best information available at the time should be the goal of top officials and their PIO staffs. The message should be consistent both within any jurisdiction or organization, and with all official public messages. The message should be delivered on a consistent and regular basis; this strategy appeared to be effective in the Maryland/Washington D.C./Virginia sniper incident and 9/11, and appeared to be effective in T2. These three elements—consistency, comprehensiveness, and the best information available at the time—are all required, and should be goals of future emergency public information campaigns.

The ability to achieve these goals in emergency public information depends upon having structured, well-defined, and robust information flow strategies, where information is accepted from pre-defined, validated sources. Such strategies do not exist currently in the national response domain, though regional JIC concepts are a critical element of such a strategy. But twenty-first century communications technologies make adhering to this critical strategy difficult as they eliminate limits of time, distance, and hierarchical structures. Ensuring accuracy of information, or at least as best as possible, depends on a comprehensive system whereby only information from identified sources is accepted as valid, regardless of whatever other information is received. A shared electronic information system could help to streamline information flow, and potentially reduce conflicting information. Ideas were raised in the seminars such as a regular news center concept and town hall meetings that may offer value as well.

The TOPOFF Exercise Series provides a unique opportunity for jurisdictions at all levels, to exercise, experiment with, and improve upon these critical strategies. T2 provided an opportunity for participants to showcase the value of concepts, such as regional JICs, that could be expanded for more comprehensive coordination at broader levels and in distributed environments (i.e., when people cannot be physically co-located). Future TOPOFFs should continue to allow participants to experiment in this area and should consider expanding on mock media functions and mock public response to further challenge participants.

This page intentionally left blank

C. Communications, Coordination, and Connectivity

1. Introduction

Nobody questions the importance of communications, coordination, and connectivity in a weapons of mass destruction (WMD) emergency response, and few would question that there are challenges that need to be overcome in this important area. These challenges are relevant in the everyday activities of Federal, State, and local (FSL) authorities, but take on critical importance during an emergency, especially one that involves WMD. While there were good practices during the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE), communications, coordination, and connectivity challenges emerged as dominant, if not the most dominant, challenges and pervaded almost every element of the response. For the purposes of this discussion, *communications* is defined as the exchange of information between agencies and jurisdictions, *coordination* is defined as agencies and jurisdictions working together to meet a common goal or to solve a common problem, and *connectivity* is defined as the means by which communication and coordination takes place. If *communication* describes the “what,” *connectivity* describes the “how.” The special topic areas provide extensive detail about many of the communications, coordination, and connectivity challenges including how they occurred, and, where possible, why they occurred.

2. Discussion of challenges and good practices

Table 16 depicts the challenges, and good practices relevant to communications, coordination, and connectivity that arose in the seminars, as well as the instances that show how these issues played out during the FSE. Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A () is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;¹³⁵ these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require continued attention of the national response community to facilitate smoother responses in the future.

¹³⁵ References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants’ opinions or did not happen.

Table 16. Communications, Coordination and Connectivity Issues during T2

ISSUES	SEMINARS/LSG					FSE INSTANCES
	Emergency Public Information	Radiological Dispersal Device	Bioterrorism	Direction & Control	Large-Scale Game Consequences	GOOD PRACTICES AND CHALLENGES
<p>a. Communication:</p> <ul style="list-style-type: none"> Processes are needed for distribution of critical information between agencies and jurisdictions and for communication of data and lab information to Incident Commander. Communication of State and local Emergency Operations Centers (EOCs) with hospitals. 	✓	✓	✓	✓	✓	<p>(-) Lack of consistent understanding of formal, validated sources for information.</p> <p>(-) In some cases, lack of formal processes/channels (or understanding of them) for official information.</p> <p>(-) Inconsistent use of terms/unclear technical language.</p> <p>(-) Burdensome/redundant reporting processes for hospitals.</p>
<p>b. Coordination:</p> <ul style="list-style-type: none"> Integration of agencies to provide unified response is not clear. Coordination across multiple agency and jurisdiction EOCs. Lack of integration of private sector and non-profit organizations in response plans. Cross-border/international coordination needed. 		✓		✓	✓	<p>(-) Multiple agencies collecting/disseminating radiological ground data in Washington.</p> <p>(+) The Principle Federal Official in both venues.</p> <p>(+) Video teleconferences (VTC) were an effective means of coordination.</p> <p>(+) In Washington and Illinois, there were several examples of EOCs working together to solve a problem (procedures for re-opening closed roads in Washington, identification of additional security personnel in Illinois).</p> <p>(+) American Red Cross participated in the Federal Joint Operations Center Consequence Management Group in Washington and at the Interagency level.</p> <p>(+) In Washington, preliminary relationships developed between businesses and emergency response community.</p> <p>(+) In Washington, Canada requested to place a liaison in the Region X Regional Operations Center (ROC).</p> <p>(+) The Department of Energy requested help from Canada on health radiation.</p> <p>(+) In Illinois, numerous examples of conference calls between EOCs and regional Federal agencies (typically the Department of Health and Human Services Regional EOC and the Federal Emergency Management Agency ROC).</p>

ISSUES	SEMINARS/LSG					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	<i>Emergency Public Information</i>	<i>Radiological Dispersal Device</i>	<i>Bioterrorism</i>	<i>Direction & Control</i>	<i>Large-Scale Game Consequences</i>	
						<p>(+) In the Interagency, many examples of Federal agencies communicating with each other.</p> <p>(-) Multiple EOCs stretch liaisons thin and can complicate coordination</p> <p>(+) Prior to the FSE, Washington Department of Health (DOH), Public Health Seattle King County (PHSKC), and EPA developed default Protective Action Guidelines for use in an RDD event.</p>
c. NEW: Connectivity.						<p>(-) In Washington, Radiation Monitoring and Assessment Center couldn't transmit data electronically; forced to use phone, fax, and courier.</p> <p>(-) In Washington, Federal Radiological Monitoring and Assessment Center used 56k modem to transmit information and courier to deliver maps to Joint Operations Center (JOC).</p> <p>(-) In Illinois, many hospital fax machines were unreliable, and there was no guarantee of successful data transfer.</p> <p>(-) Hospital data were largely paper-based and disparate reporting processes were burdensome.</p> <p>(-) In Washington, inadequate VTC capability at JOC.</p>

a. Communication

To the extent that effective coordination depends on a common information baseline, communication issues are addressed. The volume of information exchanged by players during the T2 FSE was extensive. More than 2,500 e-mails alone were courtesy copied (as requested of participants by the T2 evaluation team for use in subsequent analysis) to the T2@amti.net address, and this is likely a fraction of the total volume of e-mails exchanged. This number does not include information exchanged by fax, phone, radio, video teleconference (VTC), in person, or obtained by participants over Websites. In response to a disaster, agencies produce multiple levels of information of various types: technical data that are assimilated into information from multiple sources, individual logs kept by staff at most Emergency Operations Centers (EOCs), organizational situation reports produced at regular intervals, summary briefings, and press releases to name a few.

Analysis of T2 communications affords a rare opportunity, albeit a limited one due to time constraints, to examine this critical element of national response in an objective and relatively comprehensive manner. Such an examination is only possible through the artificiality of an exercise that permits collection of the information flow that would be impossible to implement in a real disaster. This analysis represents the highest-level assessment of this critical area. Further examination of this area is strongly recommended to help the national response community understand the existing information system upon which their situational awareness depends, including the key information nodes, along with redundancies, gaps, or efficiencies.

During T2, there were two overarching communication issues:

- Lack of formal processes/channels (or understanding of them) for official information and lack of consistent understanding of formal, validated sources for information; and
- Use of inconsistent or technical language.

Lack of formal processes/channels (or understanding of them) for official information

A prevailing issue that emerged during T2 was the lack formal processes or channels for official information. In an environment of instantaneous information access through e-mail, pagers, instant messaging, and cell phones, adhering to a structured process for exchanging information is difficult. Structured processes may be slower than informal processes; however, they are a far more effective way of validating information than numerous informal processes. When validated information is critical, it is equally critical that mechanisms exist for exchanging it.

During T2, this played out in numerous ways. Agencies experienced difficulty in validating the status of the alert level for nearly 12 hours due in part to the absence of a consistently understood process for official notifications in this arena. As described in “Alerts and Alerting” in the *Special Topics* section, many agencies learned about the Department of Homeland Security (DHS) elevations through the Virtual New Network rather than through official channels. This led to substantial efforts to confirm and validate this information.

Some agencies attributed information problems to too many official reporting channels—various agencies having their own, independent procedures and redundantly requesting updates from agencies. Public health authorities in Illinois required updated resource reporting every three hours in the midst of the outbreak. In many cases, different agencies [(e.g., Illinois Department of Public Health [IDPH], Illinois Operations Headquarters and Notifications Office [IOHNO])] requested similar information in various formats from hospitals. These cumbersome reporting processes appeared to divert resources from other priorities.

The Federal Bureau of Investigation (FBI) Strategic Information Operations Center (SIOC) is staffed by liaisons from other Federal agencies. They are there to field questions, receive information from the FBI to pass back to their agency headquarters, and provide information to the FBI from their agency headquarters. However, in many cases during the FSE, agencies directly contacted the FBI information control officer for information rather than their own liaisons. This was particularly true of DHS.

T2 provided an unprecedented opportunity for traditional government response agencies to interact and work with the public health and medical communities. Hospitals reported that they established many positive working relationships with many FSL agencies. However, they

reported that numerous calls from a variety of people from the same Federal agencies caused some confusion.

Agencies spent substantial time validating rumors about transportation closures, patient numbers in both venues, casualty figures from the radiological dispersal device (RDD) scene, and others due in part to a lack of understanding of validated sources. For example, in the Washington venue, on-scene responders were repeatedly asked about the number of fatalities. Partly because of the “fog” and urgency of a disaster, responders attempted to provide what they knew, rather than defer to the Medical Examiner,¹³⁶ leading to inconsistent estimates of the number of dead. In other cases there was a lack of understanding by official sources as to the complete list of information consumers. Both contributed in to a “whisper down the line” phenomenon as information was passed from primary recipients through secondary channels to others who passed it along, unintentionally altering the information along the way as in the childhood game “Telephone.”

Finally, there is some evidence to suggest that although many agencies, including DHS, initiated regular reporting intervals, not enough agencies did this. Those that requested “on-demand” reports often did not allow staff sufficient time to gather information. For example, a Department of Health and Human Services email notes that:

A request was made by the FBI Consequence Management Group Leader to have each agency provide talking points for a report to the Principle Federal Official, who will update the President of the United States. We had about 10 minutes to pull this information together, so I contacted ROC [Regional Operations Center] and REOC [Regional Emergency Operations Center] for assistance.

While this individual sought out official sources for information, a ten-minute notice for updates across all major elements of a disaster response is a recipe for potential information issues.

Inconsistent use of terms/unclear technical language

The use of inconsistent language proved to be another communications challenge during the T2 FSE. In the Washington venue, confusion arose with the interchangeable use by many of the term *casualties* to mean both *fatalities* and *injuries*, or both. The “Emergency Public Information” discussion in the *Core Areas* section details some additional issues with the usage of language for public information. Some of these same examples were issues in internal agency communications. Specifically, the general reference in internal agency communications to the plague resulted in at least one instance of a public health person giving advice that applied to Bubonic Plague (preparing information to reduce transmission through rodent population) rather than Pneumonic Plague. Officials remarked about the critical importance of having technical data translated into plain language to support decision-making and risk communications.

b. Coordination

In the Illinois venue, the greatest challenge involved the coordination of actions, information, and data flow requirements among 64 hospitals, five POD hospitals, and three separate but inter-related state-wide organizations (IDPH, IOHNO, Illinois State EOC). In Washington, there were

¹³⁶ In Washington, the Medical Examiner is the formal source for confirming deaths.

many agencies collecting radiological ground data to assist in the determination of the extent and type of contamination caused by the RDD explosion. Early on, these agencies transmitted their data on-demand to numerous other agencies—in many cases by-passing the coordination processes and mechanism of the Federal Radiological Monitoring and Assessment Center (FRMAC). In some cases, these agencies were measuring slightly different things, though such differences were not necessarily understood by the recipients of this information, many of whom were not technical specialists. This proved to be problematic later on when these data were used by several different agencies to create inconsistent plume and deposition models.¹³⁷

At the RDD site in Washington, there were some issues with the apparent lack of a unified command structure during the early stage of the response. Although, there were a number of briefings attended by the Seattle Police Department (SPD) Incident Commander, the Seattle Fire Department (SFD) Incident Commander, the FBI, and the Federal Emergency Management Agency (FEMA), there was no mention of a unified command to facilitate coordination efforts until 0915 on May 13, 2003.¹³⁸ However, even that briefing did not include representatives from health or emergency medical services, leaving full coordination nearly impossible.¹³⁹ A data collector commented after the exercise:

While all disciplines were present, there was no indication that they were truly working together. In fact, except for the briefings, the only interdisciplinary coordination occurred by “chance meetings...”

An additional coordination problem arose with the DHS National Operations Center and the Washington State EOC regarding deployment of the DHS Prepositioned Equipment Package (PEP). On the second day of the FSE, the Incident Commander requested deployment of the PEP. Per the guidelines in the DHS/ODP PEP Briefing Book, a request for deployment of PEP from the Washington Governor, was processed through the Washington State EOC. The data show that attempts were made to follow established PEP guidelines; however, the guidelines were vague and did not provide sufficient detail. For example, the request for deployment must come from the Washington Governor, but it was not specified if a verbal request is sufficient or if the request should be in writing. The request was eventually routed through the FEMA liaison in the Washington State EOC. However, once the request reached the DHS National Operations Center, it was not processed because the responsible individual(s) or PEP Program staff could not be located. Additionally, the staff in the DHS Homeland Security Operations Center (HSOC) appeared not to be familiar with the PEP program or process. Thus, a major delay in deployment of the PEP was encountered, while the National Operations Center tried to locate someone who knew about this program. More detailed procedures employing the HSOC as the request point of entry and training from DHS for requesting deployment of the PEP could help to ameliorate this in the future.

¹³⁷ For more information, see “Data Collection and Coordination” in the *Special Topics* section.

¹³⁸ It is possible that a unified command was established before this time, but the evaluation team does not have any such data.

¹³⁹ It is also likely that this briefing or any other at this level did not include representatives from the technical agencies collecting radiological data since they were working for the Hazardous Materials Chief, not the Incident Commander. For more information, see the *Special Topic* on data coordination.

The presence of the Principle Federal Official (PFO) in both venues, but particularly in the Washington venue, proved to be an effective conduit for improving coordination among the multiple agencies and multiple governmental levels of response. Other good practices in coordination during the FSE included the following:

- There were several examples of agencies and jurisdictions coordinating to solve problems. For example, in Washington, the Seattle EOC worked with the Washington Department of Transportation and the Washington State Patrol to develop and implement a plan to decontaminate and re-open highways. In Illinois, the EOC structure proved valuable when the State EOC activated Illinois law enforcement mutual aid to provide Chicago additional security personnel in anticipation of a shortage of city workers;
- There are numerous examples in both Washington and Illinois of State, county, and local EOCs conducting conference calls and VTCs. In many cases, these conferences included regional representation of Federal agencies, including the regional FEMA Regional Operations Center (ROC). In both venues, the PFO also initiated regular conference calls with State and local top officials.¹⁴⁰ In the Interagency venue, both the SIOC and the DHS collected information from and distributed information to other Federal agencies. Federal agencies and departments also participated in conference calls and VTCs involving many different departments and agencies and communicated between agency headquarters in Washington, D.C., and their regional counterparts;
- During the FSE, there were several good practices of standardized information sharing. All FSL agencies with permission to access the Department of Energy (DOE) National Atmospheric Release Advisory Capabilities secure Internet site could download predictions of the radiological plume. Also in Washington, the Seattle and State EOCs shared information through an Internet-based system. However, neither the King County EOC nor Federal agencies had access to the system, which limited its value. In Illinois, DuPage County utilized the Pro-Net surveillance system to track hospital calls and admissions and to provide early alerts to possible disease outbreaks; and
- The FSE provided unusual opportunities for the inclusion of some organizations not typically included in response organizations. In Washington, the American Red Cross staffed the Seattle, King County, and Washington State EOCs, which is not unusual; however, they also staffed the Federal Joint Operations Center (JOC) which was unprecedented. Their national headquarters was also involved at the interagency level. Also in Washington, the Bank of America co-located an EOC with the Federal Reserve. Finally, the months of planning allowed Seattle businesses to develop or broaden relationships with the emergency response community. They are now in the process of establishing the Business Emergency Network (BEN) to increase the business community's awareness and involvement in emergency response.
- The need for advance coordination among agencies, such as the CDC and FDA, on the availability of medical countermeasures for humans and animals for other potential threat agents is critically important. The TOPOFF Exercise Series offered numerous opportunities to do this.

¹⁴⁰ For more information, see the *Special Topic* on the Principle Federal Official.

Exercise activities that took place in Canada are beyond the scope of this AAR, but there were several examples of U.S. communications and coordination with Canadian authorities. The International Office within DHS communicated regularly with Canadian government officials as well as government officials from other nations. In addition, after the RDD explosion, DOE Headquarters requested radiological assistance from Canada. As a result, Canadian officials asked to place a liaison in the Region X ROC.

c. Connectivity

A variety of means were used to communicate during the FSE. While there was an increasing use of Internet-based transmissions, there continued to be heavy reliance on faxes particularly in the case of the Illinois hospitals. Table 16 provides examples of some of the typical connectivity issues that arose during the exercise. An issue of concern at the federal level not indicated in the table was the difficulty some agencies had receiving and passing classified information.

One issue that was not identified during the seminars or the Large-Scale Game was the potential for technical challenges. During the FSE several such challenges arose. In Washington, the Department of Health Radiation Monitoring and Assessment Center had poor connectivity and was forced to distribute data primarily via phone, fax, and with a courier. The DOE FRMAC in Washington communicated with and transferred information to their servers in Nevada through a 56K modem, which they reported as much too slow and unreliable. The Advisory Team¹⁴¹ also had technical limitations—they had one phone line, which was also their Internet connection.¹⁴² In addition, the Federal JOC in Washington had inadequate VTC capabilities. All of these connectivity challenges had an impact on the ability of technical experts, agencies, and jurisdictions to communicate effectively.¹⁴³

In Illinois, the lack of a robust emergency communications infrastructure was manifest by a reliance on telephones and faxes for patient data transmission. Often, however, the fax machines were unreliable and there was no certainty that the transfer was successful, or there was inadequate staff to monitor them. In addition, if the phone lines were compromised, then the distribution of data would be severely compromised.¹⁴⁴ While in some cases, these connectivity issues may have been due to the fiscal and physical constraints of the exercise, this was not always the case. Many organizations referenced the critical need for better, more robust connectivity (i.e., internet access) in their Lessons Learned reports.

3. Conclusion

As described in detail in the *Special Topics* section, the communications, coordination, and connectivity challenges had an impact on the information available to top officials, which in turn affected their ability to make decisions. In all three venues, top officials made decisions based

¹⁴¹ The Advisory Team consists of representatives from Federal agencies and provides the lead Federal agency with advice on environmental, food, health, and safety issues that arise during and from a radiological emergency.

¹⁴² The Federal Radiological Monitoring and Assessment Center and Advisory Team informed the evaluation team that these technical limitations are real-world—not exercise artificialities, as they set up wherever they find appropriate space. They reported working toward a mobile, high-speed system, but they have to be sure that it meets their technical and security needs.

¹⁴³ Because of a lack of coordination observed during the FSE, the connectivity challenges discussed above are the not the primary cause of the communication challenges observed during the FSE. For more information, see “Data Collection and Coordination”, “Hospital Play”, and Decisions Under Uncertainty” in the *Special Topics* section.

¹⁴⁴ For more information, see the *Special Topics* section on hospital play.

upon inconsistent and often incomplete information. Such inconsistencies also made it to the public (see the *Core Area* on public information), which has the potential to compromise the credibility of top officials. While better coordination and communications may not lead to better decisions, top officials should be confident that they are basing their decisions upon the most up-to-date and valid information available. Although it is doubtful that communications, coordination, and connectivity will ever be perfect, exercises, including the TOPOFF Exercise Series, can serve to identify areas where communications, coordination, and connectivity can be improved.

Although there were significant communications, coordination, and connectivity challenges during the FSE, players and planners reported that the building-block process allowed them to develop new or stronger relationships with their colleagues. Many have developed and implemented processes based upon their T2 experiences to improve their communications, coordination, and connectivity capabilities.

This page intentionally left blank

D. Jurisdiction

1. Introduction

Metropolitan-area providers of emergency services typically have interlocking mutual-aid agreements or emergency assistance compacts that clarify jurisdictional issues. But terrorist attacks using weapons of mass destruction (WMD) bring into play entities and considerations not normally encountered and not necessarily provided for in these agreements. Authorities that seem clear on paper are not always as clear in practice as real-world experiences and exercises repeatedly demonstrate. Previous exercises, such as Top Officials (TOPOFF) 2000, and real-world events, such as 9/11 and the anthrax attacks in 2001, highlighted such challenges. In this section, we examine the issues, conflicts, or gaps in jurisdictional authorities and the assumptions that arose when policies and agreements were put into practice under the uniquely challenging conditions of simulated terrorist WMD attacks.



2. Discussion of challenges and good practices

Participants raised and examined jurisdictional issues throughout the cycle of T2 including the FSE. Table 17 depicts the challenges, and good practices relevant to *Jurisdiction* that arose in the seminars, as well as the instances that show how these issues played out during the Full-Scale Exercise (FSE). Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A () is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;¹⁴⁵ these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require continued attention of the national response community to facilitate smoother responses in the future.

During the T2 FSE, there were many successes in the jurisdictional arena; however, the issues that were experienced emerged in two overarching areas:

- Confusion over who has authority for what actions/decisions; and
- Authority for the control and dissemination of information.

¹⁴⁵ References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

Table 17. Jurisdiction Issues during T2

ISSUES	SEMINARS/LSG					FSE INSTANCES
	Emergency Public Information	Radiological Dispersal Device	Bioterrorism	Direction & Control	Large-Scale Game Consequences	GOOD PRACTICES AND CHALLENGES
a. Confusion over roles and authorities. Some agencies seem to have duplicative roles under certain circumstances. Plans are sometimes duplicative, or in conflict. Some authorities are unclear in bioterrorism response.	✓	✓	✓	✓		() Issues during the Full-Scale Exercise were less about disputes over who's in charge, but rather <i>who is in charge of what</i> . (-) Questions arose concerning the department of Homeland Security and its relationship with other agencies. (-) Some questions with implications of bioterrorism and the declaration of a public health emergency. (-) Some uncertainty regarding transportation authorities.
b. Authorities to release information.	✓	✓		✓		(+) Regional Joint Information Center concepts implemented. (-) Frustration at Federal agencies releasing "local" messages. (-) Control of information can have an impact on other activities. <i>See "Emergency Public Information" core area.</i>

a. Confusion over roles and authorities

The primary question relating to jurisdiction during the T2 series of activities evolved throughout the exercise cycle from *who is in charge* to *who is in charge of what*. Participants increasingly clarified that the issue in emergencies is often not turf battles, but rather uncertainty among the various entities involved in response to multiple, sometimes overlapping, authorities that are driving the numerous actions being simultaneously and urgently addressed. From a jurisdictional perspective, many things went more smoothly during T2 than participants expected. For example, during the post-FSE tabletop held in Seattle, the spokesperson from the City of Seattle stated: "During T2, I expected to see a chaos of power that would hamper the response effort—these expectations were profoundly unmet as all levels of government and agencies came together to respond to this crisis." This was exemplified by the transfer of control

of the RDD site in Washington, first to the Federal Bureau of Investigation (FBI) once Seattle Fire Department completed rescue and recovery operations, and then through the Federal Emergency Management Agency (FEMA) back to the local authorities when the FBI completed the crime scene investigation.

However, beyond the RDD incident site there were instances of agencies not knowing who had what authority to make certain decisions (see the “Emergency Decision-making and Public Policy” *Core Area*). For example, in Illinois there were multiple discussions regarding who was in charge of the decontamination process, who had the authority to re-open the facilities where plague was released (the United Center, O’Hare International Airport, and Union Station) and who had the authority to define the requirements that must be met to re-open the contaminated sites. This last point is particularly troublesome since it involves both an assessment of when it is scientifically “clean” versus be perceived as safe by the public. This issue was also relevant in Washington as long-term remediation and restoration of areas with radiological contamination is a significant public health and environmental protection challenge. These, and other long-term issues, were discussed among Federal, State, and local (FSL) agencies and departments in WA at the post-FSE tabletop on May 15, 2003.

Jurisdictional authorities related to transportation were also unclear during the FSE. During T2 some confusion arose among participants as to who had what authorities to close and re-open airspace, rail systems, and road systems. In the case of airspace, there was some confusion as to whether authority to close and re-open airspace and temporary flight restrictions lay with the newly-created Transportation Security Administration (TSA) or the Federal Aviation Administration (FAA). TSA and Veterans Administration logs indicate that TSA implemented a shutdown of airspace in the Seattle area, restricted flights, and closed airspace within 30 miles of the three area airports. Other logs from FEMA, Department of Transportation (DOT) Crisis Management Center, and FAA indicate that only FAA had this authority. There was also confusion regarding the authority to close airports. Some participants, including those from FEMA, believed that only DHS had this authority. In fact, the local airport authority has jurisdiction over the status of their local airports.

Discussions occurred within DOT about the legal authority of TSA to close rail systems (currently only private rail operators have this authority for freight, while DOT has some influence over Amtrak). In addition, FEMA reported to DHS that the U.S. Coast Guard (USCG) had closed down the Port of Chicago, and a DHS Crisis Action Team (CAT) log noted that the Customs and Border Patrol had closed the Port of Seattle—when actually, only the Captain of the Port has this authority (a USCG log notes this). The USCG clarified the authorities of the Captain of the Port at the Washington venue Hotwash noting that “knowledge of these authorities would be very helpful to emergency responders.” These USCG authorities—to close the port, stop all work at all waterfront facilities, control all vessel movement including freezing them in place, to order vessels to leave, and require significant increases in security at private waterfront properties—take on potentially national and international significance within the context of a terrorist WMD attack.

There were also some issues about who could re-open road systems. In Washington, the City of Seattle’s Mayor was anxious to restore the city to normalcy as soon after the attack as possible, and publicly announced that the roads would be opened at a specified time. However, this announcement had not been coordinated with the WA DOT, which has the statutory authority for these decisions. Based upon the guidance of the WA State Department of Health (DOH), WA

DOT did not agree with the Mayor's decision. The issue was coordinated and resolved in the end but led to hours of confusion by many agencies as to the status of major highways in the area.

The FSE provided a valuable opportunity to identify and explore potential jurisdictional questions relating to DHS' the newly merged federal assets. For example, in Illinois, some issues arose with the declaration of a public health emergency by the Department of Health and Human Services (HHS). Such a declaration gives HHS the authority to deploy resources on its own initiative and at its own cost. This led to some confusion among agencies concerning the status of the Strategic National Stockpile (SNS). The decision to deploy the SNS is made by DHS in coordination with HHS. During T2, the HHS headquarters and DHS officials both gave directives regarding the SNS; SNS deployed based on DHS directives. There was no apparent coordination between DHS and HHS headquarters regarding activation and deployment of the SNS; rather, coordination occurred between senior CDC and FEMA officials. This level of coordination limits the ability of both departments to effectively manage the full scope of assets available for the response effort.

DHS now maintains many of the medical response assets formerly maintained and managed by HHS such as the SNS and the NDMS. HHS is the lead technical agency for public health and medical emergencies, yet retained few operational assets to respond to such emergencies following the creation of DHS. Furthermore, the medical expertise required for effective management of these assets is split between the two departments. It is not clear from the FSE whether this would impact HHS' ability to manage a response following a declaration of a Public Health Emergency in the absence of a presidential disaster declaration—given that it doesn't retain operational control of response assets. Further, the FSE did not stress the federal system enough to analyze how difficult decisions regarding allocation of health and medical assets would be made.

FEMA Headquarters was challenged to refine their relationship with their new parent Department, DHS, during the FSE. One email suggested that the FEMA Emergency Support Team (EST) was not included in a teleconference with the DHS CAT and therefore was kept out of the loop regarding the response. In addition, the EST felt that DHS was deploying assets without going through the proper notification channels. Furthermore, the roles and responsibilities of the new DHS Principle federal Official (PFO) are not well-defined relative to the FEMA Regional Directors and the Federal Coordinating Officer (see the "PFO" *Special Topic*). The Environmental Protection Agency (EPA) also noted in the Washington venue Hotwash the need to work through and define EPA and DHS authorities and to define who has jurisdictional responsibility to take leadership of developing and maintaining health and safety plans for all of the different entities involved. EPA also noted that the process and jurisdictional roles in tasking partners for support was unclear at times. EPA can respond to a local fire department under the National Oil and Hazardous Substances Pollution Contingency Plan, but during the FSE, the regional EPA office felt pulled by the national command structure to coordinate their response with the Federal response

Finally, while these were not played out during the FSE, some agencies did highlight potential jurisdictional issues that may have been faced in the longer-term recovery phase. EPA raised concerns at the Washington venue Hotwash in regards to balancing crisis and consequence management, especially in the context of ensuring worker safety at the site, and the potential safety of citizens on/near site. In the aforementioned tabletop exercise in Washington on May

15, 2003, agencies noted uncertainty as to who makes “large, expensive” decisions regarding restoration of infrastructure such as waste-water system and roadways that cross jurisdictional boundaries. In another example, local police acknowledged during the Washington venue Hotwash that while jurisdiction went well overall, there were some questions relative to FEMA in the recovery stage, such as “would FEMA be in charge [of] the field?”

b. Authority to Release Information

The authority to release information and the “authoritativeness” of that information was a dominant issue during T2. Leading up to the FSE, participants had focused largely on this issue with respect to public information, noting concern in numerous seminars about jurisdictions “speaking” beyond their jurisdictional boundaries. This is especially problematic when a disaster crosses jurisdictional boundaries, as was the case in both the RDD and bioterrorism attacks. As DuPage County pointed out in its Lessons Learned report, “political problems existed with multi-jurisdictional release of information, especially with varying levels of government.” DuPage County noted that these issues were amplified when Washington State issues came into play. As participants at the After Action Conference noted, the public will not know which source to believe when government officials release conflicting information.

Regional Joint Information Center concepts can help to mitigate these issues, as was seen in the Illinois venue and as was implemented on a more limited scale in the Washington venue. Broader joint information systems concepts offer the potential to strengthen this public information coordination to proactively include geographically disparate partners. During T2, there were some instances of Federal agencies appearing to release messages without coordinating fully with State or local officials. These issues are discussed in more detail in the *Emergency Public Information* core area.

An additional issue not discussed in the seminars or Large-Scale Game (LSG) arose during the FSE and concerned the “authoritativeness” of information. This issue refers to the reality of multiple agencies collecting and exchanging numerous types of information in any response effort, and the critical ability of agencies to understand who the authoritative sources are for what information.

In the Washington venue, there was confusion with the coordination of radiological data by multiple agencies—all of whom had some authority for the data they were collecting, but the result was confusion among the many agencies that received these data and were uncertain which information was correct or “authoritative.” Similar confusion was experienced by agencies sending and receiving the various plume models and projections that were developed during the FSE; some of which was caused by a lack of understanding as to who was the authority for this information. Interestingly, numerous data collector logs suggest that those agencies that generated their own models knew that the DOE was the lead technical agency in Washington. But, when asked whose model everyone should be using, most agencies answered simply that theirs was the valid one.¹⁴⁶

In another instance, agencies experienced frustration obtaining ground truth on numbers of injuries and fatalities at the scene of the RDD blast. Multiple organizations were requesting updates on this information from public health authorities and incident command, which were in

¹⁴⁶ For a more detailed explanation of the multiple plume models, see the data coordination story in the *Special Topics* section of this After Action Report.

turn receiving updates from on-scene responders. But these various sources all had conflicting information. Public Health Seattle/King County (PHSKC) noted at the venue Hotwash the importance of defining key, credible sources of information that they can rely on since people look to PHSKC for answers. It noted that it is only Medical Examiners who can officially declare deaths, but official certification may not come for days in the event of an RDD explosion. PHSKC highlighted the need to find an appropriate way to provide messages about death counts that are yet to be confirmed by the medical examiner.¹⁴⁷

3. Conclusions

The FSE demonstrated that jurisdictional policies and the extent to which they are understood by various entities drive and influence every element of response. They define what actions agencies believe they are supposed to take. T2 demonstrated the critical importance of clearly defining and understanding informational authorities as well.

Participants at all levels of government continue to state that exercises such as TOPOFF remain one of the most effective means to convey these understandings and to clarify authorities that may appear clear on paper but which are not as clear when implemented under the complex conditions of crisis. The WA State Adjutant General summarized jurisdictional challenges and solutions at the post-FSE tabletop held in Seattle, when he stated, “our issues are multi-dimensional, and not confined to any single jurisdiction—our recovery architecture must recognize non-traditional partners.”

Reiterating the critical importance of continuing to refine the collective understanding of jurisdictional authorities, the WA State Adjutant General encouraged all jurisdictions to “do serious introspection on TOPOFF, use it as stage, and pull together multi-jurisdictional functional areas to talk about what worked well throughout that pulsing system and take a hard look at the gaps at the seams.”

¹⁴⁷ Mass fatality management and casualty tracking was a real world problem during the response to the Oklahoma City bombing and the 9/11 attacks. The Department of Homeland Security, Office for Domestic Preparedness, produced a document that discusses these issues.

E. Resource Allocation

1. Introduction

Resource Allocation challenges require decision-makers to weigh conflicting needs and determine how best to apportion limited resources. The conflicting needs can challenge decision-makers within a single agency, or can force decision-makers from different agencies and departments to work together to decide how best to manage critical resources that are in short supply relative to the demand. Often the solution is unconventional.



A weapons of mass destruction (WMD) event producing mass casualties could put enormous demands on scarce medical and public health resources. Resource issues would likely have become a concern in the Washington venue as part of the long-term recovery, post-Full-Scale Exercise time period.

2. Discussion of challenges and good practices

Table 18 depicts the issues, challenges, and good practices relevant to *Resource Allocation* that arose in the seminars, as well as the instances that show how these issues played out during the Full-Scale Exercise (FSE). Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A () is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;¹⁴⁸ these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require continued attention of the national response community to facilitate smoother responses in the future.

¹⁴⁸ References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

Table 18. Resource Allocation Issues during T2

ISSUES	SEMINARS/LSG					FSE INSTANCES
	Emergency Public Information	Radiological Dispersal Device	Bioterrorism	Direction & Control	Large-Scale Game Consequences	GOOD PRACTICES AND CHALLENGES
a. Lack of consistent understanding among Federal, State, and local (FSL) agencies of what federal resources are available, how to request those resources, and how much is available.			✓			<p>(-) Confusion over official channels to acquire the Department of Health and Human Services (HHS) assets now at the Department of Homeland Security (DHS).</p> <p>(-) Local agencies did not always know which capabilities were available for request.</p> <p>(+) Officials elicited actual requirements through teleconferences.</p> <p>(-) Confusion over the process for declarations and in some cases the federal assistance they trigger through the Stafford Act.</p> <p>(+) Coordination of resources in the State of Illinois to secure sufficient security personnel via Emergency Operations Centers.</p>
b. Planning for effective use of resources in emergencies.			✓			<p>(+) Pre-planning the Strategic National Stockpile distribution sites.</p> <p>(+) Supplementing medical personnel with school nurses.</p> <p>(+) Preplanning stockpiles of antibiotics.</p> <p>(-) Multiple agencies reserved a key distribution site.</p>
c. Handling shortages of limited resources.						<p>(+) Illinois Governor's emergency orders opened up sources of volunteers.</p> <p>(+) The American Red Cross tapped supplemental sources to offset shortages.</p> <p>(-) In the Washington venue, FSL resources would have been stressed during the recovery phase, but weren't played out during the exercise.</p> <p>(+) DHS concerned with the long-term impact of nationwide red alert on resources.</p> <p>(+) HHS concerned with the long-term and widespread impact of pneumonic plague.</p>

a. Lack of consistent understanding among Federal, State, and local (FSL) agencies of what federal resources are available, how to request those resources, and how much is available

During the Full-Scale Exercise (FSE), confusion was observed at local and state levels about federal assets and the processes for obtaining them. A few examples are highlighted here; more details on this particular issue are explored in the “Proclamations and Declarations” and the “Strategic National Stockpile (SNS)” *Special Topics* sections in this AAR.

There currently is no single source to help state and local emergency managers or responders to determine which federal resources would best meet their needs during an emergency, and there are many methods by which State and local governments can request federal resources. During the T2 FSE, States often requested specific assets—sometimes requesting inappropriate or unnecessary assets in error. For example, in Illinois a request was made for Disaster Medical Assistance Teams (DMATs), although assistance from mortuary services and epidemiologists was desired. On a positive note, this disconnect was identified and corrected during a conference call among the city, state, and regional Federal operations centers.

In the State of Washington, the evaluation team did not identify any examples of such confusion. There are a number of possible reasons for this. One possibility is that Washington has its own radiological emergency experts, as well as experience with radiological emergencies and exercises involving nuclear power plants. Thus, Washington State emergency responders are able to draw upon existing knowledge, experience, and relationships.

In both the States of Washington and Illinois, there was evidence that State and local agencies made requests to the Federal Government based upon *what* and *who* they knew, and, that State and local governments do not know all of the federal resources that are available. These informal methods are not the most efficient way to obtain the necessary resources, and in some cases did not result in the most appropriate resources for the task.

There are many methods by which federal assets can be requested. Requests can go directly to agencies, or federal departments including the Department of Homeland Security (DHS) once they are involved.¹⁴⁹ Because resources are requested and deployed from different sources, it can be difficult for the Federal Government to track and coordinate the many federal assets in the field. This can make it challenging, if not impossible, for decision-makers to weigh all of the available information about resources as they become depleted because the decision-makers might not have complete information on what remains available.

This is not to suggest that the many processes for requesting assistance be replaced with a centralized system. In fact, these multiple avenues for requesting assistance are critical for a number of reasons, including situations for which disasters are not declared, and for ensuring that assets arrive at disaster scenes before official Presidential Declarations are signed—the latter of which occurred during T2 (e.g., Seattle Fire Department requested assistance from EPA not long after the explosion, and Washington State made a direct request to DOE to deploy the Federal Radiological Monitoring and Assessment Center (FRMAC)). FEMA currently tracks and reports the use of federal assets in a disaster through its Mission Assignments and Situation Reports, but

¹⁴⁹ It is currently unclear, or possibly undetermined, whether such requests should go through Federal Emergency Management Agency and the Federal Coordinating Officer, or through the designated Principle Federal Official (PFO) or delegate. See the *Special Topics* section on the PFO for more information.

distribution of these reports is fairly inefficient—usually transmitted through e-mail or fax. There does not appear to be a “one-stop shop” where FSL agencies can obtain information regarding the range of assets that are available, how to obtain those assets, or the status of assets once deployed. A web-based, searchable database of all available federal resources (potentially expanded to include state and local resources at some point), including their names, acronyms, capabilities, and request processes—a distributed yet coordinated knowledge base—may be helpful and may also minimize personnel requests based solely upon “what and who” an individual knows.

b. Planning for effective use of resources in emergencies

Planning prior to the FSE¹⁵⁰ appeared to facilitate some of the FSE activities. In Illinois, planning for receipt and distribution of SNS medications resulted in a fairly smooth-running process. In contrast, shipment and distribution of the Strategic National Stockpile¹⁵¹ did not go as smoothly in the TOPOFF 2000 exercise. This reflects in part the tremendous investment in planning and preparedness that has occurred in state and local public health departments since the fall of 2001. In particular, bioterrorism preparedness grants awarded by HHS to state public health departments in 2002 spurred the development of SNS distribution plans among many other activities. The success of the SNS distribution during T2 provides one of many examples of how potential improvements in the nation’s emergency response system can be examined in the TOPOFF Exercise Series.

c. Handling shortages of limited resources

A shortage of prophylaxis for first responders coupled with a concern for unusually high absentee rates led Chicago area officials to predict a shortage of personnel available for security. When the City of Chicago requested security support from the Illinois National Guard, they learned that this resource was unavailable—the troops were deployed in Iraq. Fortunately, the city was able to obtain the needed security personnel from neighboring jurisdictions through existing mutual aid agreements. While this met Chicago’s short-term needs, it is not known whether this solution would be sustainable over a greater time period, as the outbreak spread and as neighboring jurisdictions recognized their own needs for security. T2 did not evolve to this level of play to allow greater insight.

Responders obtained via mutual aid agreements also supported Seattle’s response. For example, the State Fire Services Mobilization Plan was mobilized to support local firefighters. In addition, Seattle had 14 engines, four ladders, and 21 police cars that were contaminated and impounded. This equipment was expected to be replaced by neighboring jurisdictions using mutual aid agreements. The mutual aid partners, however, were concerned about the length of time that Seattle would need the loaner equipment. This concern was especially relevant because unions told Seattle (notionally) that they would suggest their members not use previously contaminated equipment. They were concerned that “clean” wouldn’t really be clean.¹⁵²

¹⁵⁰ The evaluation team is not privy to whether this planning was specific for the T2 exercise, or whether it is consistent with real-world planning for emergencies.

¹⁵¹ The National Pharmaceutical Stockpile was renamed the SNS when it became part of DHS.

¹⁵² Note that the definition of clean/decontaminated was brought up in seminars, the LSG, and in the Washington venue tabletop exercise. In these discussions, players were not convinced that the public would be comfortable with places and equipment deemed “safe” after decontamination.

In some cases, it is possible to circumvent potentially limited resources by expanding the resource pool. During T2, this circumvention was done in two ways: 1) by relying on unconventional sources of support, and 2) by intervening with executive orders that exempt individuals from repercussions (often legal battles) that would otherwise prevent these individuals from providing services. For example, the American Red Cross requested mental health counselors from the Chicago Public School system to fill in for its predicted 20 percent absentee rate. Also in Illinois, the Governor signed several emergency executive orders that restricted liability and provided immunity to people supporting the response. One was particularly valuable for SNS distribution: it allowed non-pharmacists to dispense prophylaxis.

One of the many challenges in managing limited resources is working to maintain enough resources to handle other yet-to-occur situations—predictable or otherwise. To meet this challenge, those who make allocation decisions need to decide what, if anything, they should hold back from immediate requests to ensure there are resources to support other needs, should they arise. Such planning requires a risk assessment, and, in the case of bioterrorism, expertise on how and how quickly the disease can spread. Such planning requires difficult choices, as it could lead to unfortunate illness and even death. However, it can also avert nation or worldwide spread of epidemics. There is evidence of such planning during T2. In one example, the DHS Emergency Preparedness and Response Directorate was working on a plan to distribute drugs from the SNS to other states that requested the stockpile, recognizing the inevitable spread of cases outside Illinois. In addition, public health officials in Illinois anticipated potential hospital surge requirements that the growing epidemic would require (see “Decision Making Under Conditions of Uncertainty” in *Special Topics*). The Severe Acute Respiratory Syndrome (SARS) outbreak has caused public health authorities to think about how to provide surge capacity. Of course, in the event of bioterrorism, an outbreak could be much more severe. In Washington, the National Guard Civil Support Team was released from the incident site and placed on standby in case they were needed to respond to another incident. Thus, officials at all FSL levels were developing plans to handle the unpredictable.

3. Conclusions

For a variety of fiscal and operational reasons, play in Washington was limited and did not fully stress the system. For example, field play ended after two days, and exercise play ended after a command post exercise on the third day (D+2). The result was that many resources that are often exhausted early in the response either did not need replacing or were not exhausted. In addition, prior to the FSE, the Washington venue chose not to play the plague scenario—which meant that the two incidents did not interact, except in terms of the criminal investigation.¹⁵³ In fact, during the exercise HHS sent at least one inject via fax to Public Health Seattle/King County (PHSKC) Department regarding plague patients. PHSKC responded that it was not playing the plague scenario because of real-world resource limitations on public health workers stemming from SARS and the smallpox vaccinations.¹⁵⁴ Players in the Washington State Emergency Operations Center commented that they would have been very challenged if they had played the plague scenario. Furthermore, levels of radiation were designed to be relatively low to impose relatively

¹⁵³ Note that early incarnations of the scenario had plague coming to Washington State, but the radiation from Seattle was never conceived of as being transferred to Illinois.

¹⁵⁴ Near the end of the exercise, participants at the King County and WA State EOCs took actions related to the plague outbreak.

minimal impact upon the community. Nonetheless, Washington resources were stressed and requests were made for assistance from mutual aid partners and federal resources. Furthermore, some federal assets, such as the FRMAC, reported that they were having difficulty meeting all requests.

In Illinois, issues of limited resources were anticipated, discussed, and planned for, often with creative and unusual solutions. Federal resource managers also predicted and planned for resource depletion through decision-making that would likely be unpopular. This type of planning suggests that the Federal Government was prepared to make difficult decisions that might be needed following terrorist events.

F. Anticipating the Enemy

1. Introduction

The existence of an enemy makes the response to terrorism attacks qualitatively different from the response to any natural or conventional disaster. For example, the desire to keep terrorists in the dark regarding response plans can work against the desire to keep the public informed. Nature is morally neutral and indifferent to its own effects. Terrorists, however, can exploit government and public reaction to an attack, and this consideration must be taken into account. Media reports, some of them quite detailed, describing adjustments being made by the Government in the wake of 9/11, were criticized for making too much information available to the terrorists. While an active Red Team during the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE) was limited in scope, the actions of responders and top officials can still demonstrate awareness of potential follow-on attacks. This area of analysis focuses on those actions discussed in the seminars and observed during the FSE that related to the need to anticipate the enemy.

2. Discussion of issues: challenges and good practices

Table 19 depicts the issues, challenges, and good practices relevant to *Anticipating the Enemy* that arose in the seminars, as well as the instances that show how these issues played out during the FSE. Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A () is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;¹⁵⁴ these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require continued attention of the national response community to facilitate smoother responses in the future.

¹⁵⁴ References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

Table 19. Anticipating the Enemy Issues during T2

ISSUE	SEMINARS/LSG					FSE
	Emergency Public Information	Radiological Dispersal Device	Bioterrorism	Direction & Control	Large-Scale Game Consequences	GOOD PRACTICES AND CHALLENGES
a. Balance public information with security needs.	✓	✓				() No evidence to support or refute.
b. NEW: Recognition by decision-makers that an active malevolent enemy may seek to exploit response strategies.						(+) Showing caution in responding to an event that might have a terrorist origin. (+) Proactively raising defenses over a widespread area after one area has had a confirmed or strongly suspect terrorist attack. (+) Development of plans to manage limited resources in the event of another attack. (-) Several agencies suggested that anticipating the enemy is not their concern or that it is the responsibility of the Federal Bureau of Investigation.

a. Balancing public information with security needs

Top officials have to weigh competing factors when deciding to release information that could be used by terrorists. These include:

- The need to anticipate the enemy's use of available information, and sometimes limiting the content of information about the response or other emergency-related activities (e.g., shelter locations) that is released to the public; and
- The need to retain the public's confidence or even to enlist their cooperation, and sometimes make statements indicative of what is known about the enemy, including their potential whereabouts, plans, etc.

b. Recognition by decision-makers that an active malevolent enemy may seek to exploit response strategies

During the FSE, there were a number of responder and top official activities that demonstrated a keen awareness of potential follow-on attacks in other U.S. locations and in the already targeted locations. Some examples include:

- Soon after the explosion in Seattle, the Seattle Federal Bureau of Investigation (FBI) field office and FBI Headquarters counter-terrorism division initiated an initial threat assessment, examining the possibility of other explosive devices in the Seattle area;

- The City of Chicago and surrounding counties increased surveillance, and decreased parking and deliveries, at pre-selected, likely terrorist targets after the RDD attack in Seattle incident; and
- Nationwide, there were various closures, and increased guards at facilities, such as nuclear power plants.

In Seattle, the National Guard Weapons of Mass Destruction Civil Support Team was released from the RDD explosion site at 1230 Pacific Daylight Time on May 13, 2003, in part so that they would be available to re-deploy in the event of another terrorist attack, at another place, and at another time. Similarly, considerable thought was given to this by the Department of Health and Human Services, the Department of Homeland Security, the Centers for Disease Control and Prevention, and others to the need to deploy the Strategic National Stockpile and other resources, with explicit mention that the Chicago metropolitan area might not be the only area attacked with Pneumonic Plague.

Finally, the increases of the Homeland Security Advisory System Threat Condition from Yellow to Orange, and then to Red, whether nationwide or only in particular cities coast-to-coast, represented the ultimate in proactively raising defenses over a widespread area.

However, many agencies and jurisdictions acknowledged that they either were not playing against an enemy or that it was the responsibility of others (e.g., the FBI and the Joint Operations Center) to consider the enemy. The former likely represents an exercise artificiality. Further Red Team play was limited to tactical support to the Seattle Police Department Special Weapons and Tactics (SWAT) team, the U.S. Coast Guard, and FBI SWAT activities in the state of Washington, as well as to the Illinois State Police and FBI Hostage Rescue Team activities in the state of Illinois. These events did not impact the broader T2 FSE, and therefore Red Team activities did not directly impact any decisions made by top officials. Yet, agencies and jurisdictions must be aware that their responders will be at risk by nature of being part of the response. The loss of responders in additional attacks could seriously impair an agency's or jurisdiction's response capability, not to mention how such a loss would impact the morale of other responders and the public at large.

3. Conclusions

Despite the fact that the exercise contained limited Red Team play, many participants did consider the possibility of further terrorist attacks. Examples of their doing so exceed the few cited here.

The question of how to respond to an event that seems to have been an act of terrorism, but is lacking conclusive proof, is problematic. This was faced on 9/11 and in the wake of the anthrax attacks in 2001. Officials need to strike a delicate balance among all the competing demands of protecting the public in both response and prevention.

This page intentionally left blank

VII. A COMPARISON TO TOPOFF 2000

This section compares Top Officials (TOPOFF) 2 (T2) to the earlier TOPOFF 2000 Exercise. TOPOFF 2000 resulted in a substantial and valuable Exercise Observation Report, which should be consulted for further details on TOPOFF 2000 findings.

A. Design

The Full-Scale Exercises (FSE) in both TOPOFF 2000 and T2 featured:

- Top official participation;
- A city with a pneumonic plague event;
- Another city with an explosion/hazardous materials (HAZMAT) event: in TOPOFF 2000 a bomb was detonated releasing a persistent chemical agent in Portsmouth; in T2 a radiological dispersal device (RDD) was detonated in Seattle; and
- Interagency play at the command post level in Washington, D.C.

Despite the similarities of design between the two TOPOFF exercises, there were major differences. T2 added an international element, not present in TOPOFF 2000, by including some international elements in the scenario and through Canadian government participation.

The designers of T2 responded to some of the TOPOFF 2000 participant feedback, most notably by:

- Facilitating the increased involvement of top officials;
- Eliminating TOPOFF 2000's "no-notice" character in favor of an open exercise in which participants were introduced to the exercise scenario through a cycle of exercise activities of increasing complexity that included seminars and a large-scale game (LSG);
- Introduction of a limited opposing force, or Red Team, to develop the concept and rules of play so that a more robust Red Team could be employed in future exercises; and
- Giving increased attention (via the LSG) to long-term recovery issues.

Exercise planners in the venues actively participated in the design of the scenario. The full-notice, "open-book" nature of the T2 FSE also helped to allay participants' concerns that they or their performance would be evaluated. However, these changes brought about some post-exercise criticism in the media that the "open book" nature of T2, including extensive exposure of the participants to the scenario in the seminars, minimized free-play decision-making. In fact, the designers deliberately chose to maximize continuous learning rather than sequestering the scenario.

This early involvement in design paralleled another path of continuous pre-FSE participation, namely that of the seminars and the LSG. These used the same scenario as the FSE (more precisely, each seminar used the FSE scenario as it stood at the time of the seminar), and had the

effect of making the participants and the designers more aware of the details of each topic treated in the seminars.

B. Participants

Despite its designation as a top officials' exercise, ("TOPOFF," based upon the term *Top Officials*), TOPOFF 2000 was assessed to have suffered from insufficient top official participation. Likely reasons include the conflict between the no-notice nature of TOPOFF 2000 and the heavily pre-scheduled commitments of top officials. In T2, top officials at all levels of government participated actively during the FSE.

The participating T2 organizations in the Washington and Illinois venues—including local, state, and regional federal entities, as well as private organizations such as the American Red Cross—are too numerous to list here, but special mention must be made of the remarkable level of participation by Chicago area hospitals. Far in excess of the number hoped for, hospitals in the metropolitan Chicago area volunteered to participate in the demanding T2 exercise, and did so while maintaining their caseload of real patients, who required real care at the same time. For this reason, T2 represented an unparalleled opportunity to examine the operation of the public health and medical communities in the face of a bioterrorism attack. This was in significant contrast to the limited medical play which occurred during TOPOFF 2000.

C. Evaluation, and the Data to Make It Possible

T2 employed a significantly different approach to exercise evaluation in TOPOFF 2000. The TOPOFF 2000 Exercise Observation Report is a compilation of the after-action reports of the individual participating entities, and the results of an after-action conference held some months after the exercise where perspectives on the exercise were obtained and exchanged. Such reports and conferences are extremely valuable, and T2 has benefited from having received such reports and having had a similar post-exercise conference one month after the FSE (held on June 17 and 18, 2003); but such information and perspectives, while valuable, are not data.

During the T2 Full-Scale Exercise (FSE), data collectors worked side-by-side with participants to document a time-based record of player actions and decisions. These, and other logs kept by exercise controllers as well as those created in the course of play by participants including emails whose work (and therefore whose FSE play), were combined and sorted by time. Entries were tagged for relevance to the six core areas of analysis and to several of the special topics whose importance emerged only as the FSE unfolded. From these records, analysts working on any particular area of analysis or topic could quickly find all relevant occurrences and compile a comprehensive look at the events sorted according to time. This allowed analysts to view the interconnections that no single participant or observer would have been able to perceive. Importantly, this process traces T2 findings back to the events that actually took place during the exercise. As such, T2 effectively represents the baseline exercise from which all future exercises can be systematically compared.

D. Findings

The following sections present a brief comparison of the results from T2 to the findings of TOPOFF 2000. In the interest of brevity, the latter are taken entirely from the TOPOFF 2000

report's 14 major areas of observation¹⁵⁵ and re-arranged to conform to T2's six core areas of analysis.

1. Emergency public information (EPI)

TOPOFF 2000 resulted in the following observations regarding public information:

- “Confusion on EPI roles, responsibilities, and appropriate public messages”; and
- “Confusion was evident in the chemical venue regarding the role of Joint Information Center (JIC) and Joint Operations Center (JOC) responsibilities.”

Confusion as to EPI roles and responsibilities for messages emerged as well in T2. For example, in Seattle a Public Information Officer (PIO) speaking for the King County Regional JIC said in a press conference that there are “no casualties” from the Seattle RDD blast when in fact the King County Emergency Operations Center had a casualty count that was over sixty, and included two fatalities. Other examples included inconsistent themes in public messages from top officials in the Washington venue regarding the relative danger from radiation; varying guidance from agencies regarding antibiotics in Illinois; and at least one press release from the City of Chicago requiring proof of presence at the suspected exposure sites as a condition for receiving prophylaxis.

The confusion of JIC and JOC roles does not seem to have been repeated.

2. Emergency public policy and decision-making

In TOPOFF 2000:

- “Authorities and guidance for population control and movement restrictions (e.g., quarantine) for a large-scale public health emergency are uncertain and not widely understood”;
- “TOPOFF 2000 highlighted the need for improved public health sentinel surveillance capabilities”;
- “The capacity to gauge the scope and consequences of a catastrophic WMD incident and convey that information to senior officials must be improved to facilitate timely and appropriate decision-making”;
- “Lack of, or limited use of, detection equipment was a significant impediment to early recognition of chemical, biological, and radiological...WMD attacks”; and
- “Updates on mitigation efforts must be widely transmitted to both responder communities and the public.”

The contrast between TOPOFF 2000 and T2 in this regard is interesting and deserves considerable attention.

¹⁵⁵ Note that TOPOFF 2000's usage of the term “observation” does not necessarily conform to the definition applied to that word in this T2 After Action Report.

As a result of substantially increased public health funding in the wake of the anthrax attacks, planning efforts directed towards a possible intentional smallpox release by terrorists, and actions taken to prepare for a potential Severe Acute Respiratory Syndrome (SARS) outbreak in the United States, considerable thought has been given to the issues of population control and movement restrictions. Despite these activities, implementing them in the event of a real-world requirement would most likely be a difficult problem. T2 did not exercise this aspect of the public health response to a disease outbreak, although policies such as *shelter-in-place* and *snow days*¹⁵⁶ were implemented to protect the population and legal authorities to restrict movement were invoked.

T2 did not fully provide an opportunity to test the efficacy of sentinel surveillance of disease and radiological detection systems. Given the large number of initially exposed individuals, the onset of the plague in Illinois was sufficiently dramatic that it prevented such a test.¹⁵⁷ At one point there had been discussion of having a more subtle disease onset in the Illinois venue to test surveillance systems, but other objectives could only be served by having a large number of patients, and those objectives were deemed more important. There were a number of attempts to estimate the scope of the plague outbreak in Illinois but this was not fully played out during the FSE. Had the exercise continued for one or two more days, the scale of the outbreak would have become a significant issue. Even so, at the federal level in the Department of Health and Human Services, efforts were underway as the week went along to determine the scope of the disease outbreak in order to assist resource planning.

In TOPOFF 2000, the responders entered the blast site and became contaminated by the chemical agent; in T2, by way of contrast, responder safety was clearly balanced against the need to rescue victims. However, officials may have been challenged if the public complained about seeing responders “hanging back” from the incident site.

The TOPOFF 2000 report cites national plans (e.g., the Federal Response Plan (FRP), and the Federal Radiological Emergency Response Plan) as needing reconciliation with Presidential Decision Directive (PDD)-39, the *Domestic Guidelines*. T2 took place in the transition to Homeland Security Presidential Directive (HSPD)-5 from the existing FRP and concept of operations. The creation of DHS and the attendant development of a National Response Plan (NRP) and National Incident Management System (NIMS) mean that the next TOPOFF exercise will be conducted under different doctrine and policies. As such, further analysis of the exercise data can provide additional valuable insight into communications, coordination, and connectivity issues that will be important in the development of the NRP and the NIMS.

Finally, since there is no real-world precedent in which the Stafford Act has been applied to a biological disaster—or one involving non-explosive radiological, chemical, or biological weapons—it is noteworthy that in both TOPOFF 2000 and T2, the widespread impacts of the biological attacks did not qualify as a “disaster,” under The Stafford Act. In T2, this led to a declaration of “emergency” in Illinois, when a declaration of disaster was requested by officials. The distinctions between the assistance that can be obtained through these two types of declarations were not always understood by participants. Future exercises should continue to

¹⁵⁶ During the T2 Full-Scale Exercise, the phrase *snow days* indicated to participants that they were to stay at home as if they had been impacted by a major snow storm.

¹⁵⁷ Although as noted in the special topic on hospital play, the initial indicator of the plague outbreak appeared to have come from DuPage County’s Pro-Net surveillance system.

refine the applicability of the Stafford Act to bioterrorism and other non-explosive disasters not explicitly defined in the Act, in order to increase Federal, State, and local (FSL) agency familiarity with its application to, and implications for, such disasters.

3. Resource allocation in TOPOFF 2000

The TOPOFF 2000 report cited shortages of medical and other supplies, and the ensuing competition over these supplies on the part of multiple jurisdictions.

The T2 scenario was designed not to stress resources to the breaking point, so shortage concerns did not generally arise. However, there was a potential prophylaxis shortage in the Illinois venue that was quickly averted by the introduction of Vendor Managed Inventory. The RDD incident was not large enough to exhaust the region's resources at least in the near term. Similarly, the exercise ended in the Illinois venue before the most challenging resource demands impacted the medical system in terms of resources such as beds, ventilators, and staff.

4. Communications, coordination, connectivity in TOPOFF 2000

The TOPOFF 2000 report recorded the following observations regarding communications, coordination, and connectivity:

- “Improved interaction is required among U.S. Departments and agencies and international organizations ... regarding alerts, notifications, and warnings”;
- “Roles and responsibilities in notification (e.g., the National Response Center) were not clear”; and
- “There was no ability to broadcast collective warnings.”

These issues remain among the most dominant challenges faced by the national response community. The creation of DHS and the development of the Homeland Security Advisory System have helped to provide communication frameworks, but numerous challenges remain. In T2 these challenges manifested themselves in numerous instances such as the elevation of the HSAS to red for the first time in an exercise or the real world, tracking patient numbers and casualties both in the Washington and Illinois venues, and coordination of public information messages in both venues. Issues remain in the areas of information access, formal and informal communications channels across multiple EOCs and with substantial use of internet-based communications, insufficient electronic communications infrastructures in some domains such as the medical community, and common language, to name a few.

5. Jurisdiction in TOPOFF 2000

In TOPOFF 2000, it was observed that:

- “Roles and responsibilities for operational direction and control...were blurred by the proliferation of response teams.”

Despite the creation of DHS, this observation might resonate with some T2 participants. In particular, the role of the PFO in regard to the previously existing response structure needs to be clarified. The proliferation of federal response teams remains an issue—there appear to have been more teams in T2 than there were in TOPOFF 2000. Coordinating and effectively using these federal assets is an area requiring attention.

Plume modeling and deposition analysis problems in T2, and associated data collection and coordination issues, can also be viewed as jurisdictional issues. Furthermore, there were jurisdictional uncertainties over who had the authority to shut down and re-open the transportation infrastructure (e.g., highway, rail, and air systems).

T2 AAR #041

VIII. EXERCISE DESIGN AND CONDUCT LESSONS LEARNED

The Top Officials (TOPOFF) 2 (T2) After Action Conference (AAC) attendees and exercise participants identified several lessons learned relative to exercise design and conduct. After assembly and review, comments were compiled into the following eleven subject areas:

- Planning, Participation, and Coordination Considerations;
- Intelligence Development and Management Processes;
- Exercise Document Guidelines;
- Exercise Time Standards;
- Exercise Artificiality Considerations;
- Consideration of a Functional Web-based Control Capability;
- Additional Exercise Event Considerations;
- Scenario Scripting Considerations;
- Virtual News Network Considerations;
- Exercise Security Considerations; and
- Coordination and Venue Design Team Empowerment.

A. Exercise Design and Conduct Comments

This section addresses exercise design and conduct comments as they pertain to each subject area.

1. Exercise planning, coordination, and participation considerations

The Secretary of Homeland Security should continue to solicit participation in the TOPOFF Exercise Series by formal invitation, encouraging the direct involvement of top officials at every level of Federal, State, and local response, including appropriate non-government organizations.

T2 AAC participants commented that invited senior officials should commit themselves and their organizational resources as early as possible. While T2 gained substantial top official involvement, future events would hugely benefit from even greater support from senior leaders. Their early and significant commitment immediately increases process relevance and the potential for exercise success. The Secretary of the Department of Homeland Security (DHS) direction in establishing a national exercise program to be administered by the DHS Office for Domestic Preparedness (ODP) will aid participants in scheduling and scoping participation in TOPOFF and other national-level exercises.

The T2 seminars included many senior officials. Comments suggested the complex process for forwarding invitations and coordinating participation requires improvement. Invitations were often forwarded within an organization's executive channels and bypassed the primary exercise planner. This process should commence well in advance of suspense dates to ensure that

exercise planners are aware and informed. Primary exercise planners play key roles in preparing senior officials for meaningful event participation.

Many T2 participants were concerned about the relatively late identification and commitment of participating organizations. Commitments to scope of participation and statements of support requirements must take place earlier in the planning process. T2 planners developed a Memorandum of Understanding (MOU) to codify and identify participating organizations, their commitment levels, and their administrative and logistical support needs. The T2 MOU was completed too late in the planning process to be fully effective. Future TOPOFF Exercise event planners should formalize this document as a binding Memorandum of Agreement completed prior to significant exercise planning and staffing expenditures, preferably by the Mid-term Planning Conference.

Participant comments suggested that T2 data collector and controller roles and requirements were not clearly defined. Qualification guidelines and more specific information regarding their duties would enable more appropriate personnel selection and application. Recruitment needs to occur early enough to permit sufficient opportunity for their training.

Several individuals and organizations suggested including past TOPOFF venue participants in future TOPOFF Exercise planning processes. Individuals with first-hand venue experience in past TOPOFF events could contribute an important depth of corporate memory and insight to future events planning.

T2 included substantial international play, primarily with Canada, reflecting the international scope of potential weapons of mass destruction (WMD) events. It was recognized that future TOPOFF exercises should emphasize more international involvement. Consideration should be given to inviting key international bodies such as the World Health Organization, in addition to other governments.

2. Intelligence development and management processes

T2 intelligence play was purposefully designed to provide background support to drive the exercise scenario. For simplicity, T2 did not provide an opportunity for analytical review and intelligence development. Several comments suggested including enough depth and complexity of notional intelligence processes to allow for analysis in real time. Such intelligence play should enable and promote the intelligence buildup at exercise commencement and continue as a robust element of play throughout the event. The intelligence community should provide answers to requests for information, including the production of “tear-lines” so that DHS can produce press releases based upon them. This would support the concept of prevention, an important aspect of homeland security.

Further comments suggested that all exercise intelligence data should be handled within actual controlled channels, as it would in the real event.

3. Exercise documents guidelines

Many participants were unclear about T2 scenario control with respect to injects. There was confusion as to which were official, and how official requests for information or injects would or should be received and processed. Most agreed that participants should use preexisting organizational document formats during exercise play just as they would in reality. These documents must include appropriate exercise caveat markings that clearly identify them as

notional so they are not confused with actual document traffic. The exercise control group should use standardized exercise document formats, recognized by all participants as exercise control documents. Establishment of the National Exercise Program and collaborative management processes will improve available tools and templates.

4. Exercise time standards

Confusion sometimes existed as to time references, particularly as the Master Control Cell was in Washington, DC (Eastern Daylight Time), and the venues were in the states of Illinois (Central Daylight Time) and Washington (Pacific Daylight Time). Comments suggest eliminating such confusion with the mandatory use of Coordinate Universal Time, or Universal Time, previously known as Greenwich Mean Time, for all exercise transmissions.

5. Exercise artificiality considerations

Exercise artificialities occur simply because many aspects of a real situation cannot be effectively simulated. The scope of exercise play is limited by funding, logistical and geographical constraints; therefore, some artificialities are beyond planner control and others are choices specifically made to enable specific exercise goals and objectives. Each artificiality should be the product of a conscious choice and provide the means to demonstrable ends. Exercise planners should clearly identify and consider each artificiality for its necessity in achieving exercise objectives.

Overall, planners must weigh real exercise factors against versus notional ones. A robust firewall between artificial scenario information and real world information must be established and maintained at all costs. Realistic deployment timelines and parameters must be maintained in cases where assets are positioned administratively to simplify logistics and costs.

Comments suggested notionalizing additional elements of future events by including first responder casualties, more aggressive exercise press coverage and media pressure, Web-based news formats, extension of play to include more long-term consequences and recovery considerations, and challenges to Continuity of Operations and Continuity of Government plans and processes.

6. Consideration of a functional Web-based control capability

A serious shortcoming cited in T2 was the failure of planned controlled access communication channels and the use of a Web-based Master Scenario Events List (MSEL) tracking tool. In short, the Extranet Secure Portal and the on-line MSEL tools did not achieve performance expectations. Such on-line exercise control tools must be fully functional and all controllers must have ready access and confidence in the tools' reliability.

7. Additional exercise event considerations

While the T2 Full-Scale Exercise (FSE) ended as planned on May 16, 2003, there may have been significant utility in a post-FSE event focusing on remediation and long-term recovery aspects leveraged from the FSE scenario and play. To exploit similar future opportunities, planners should consider the potential of post-FSE events to produce a more comprehensive learning experience. Other smaller spin-off precursor or successor events could emphasize prevention

and protection aspects of a WMD terrorist incident as well as response, and engage all potential players during a notional intelligence buildup.

8. Scenario scripting considerations

Future exercises must closely balance scenario scripting against free play. It is important that all controllers clearly understand the definition and function of the MSEL and Procedural Flow (PROFLOW) processes. To avoid the premature disclosure of MSEL information that occasionally occurred during T2, future events should re-emphasize limited access and distribution of MSEL/PROFLOW information, and establish voluntary yet firm non-disclosure policies. An organizational exercise planner is a “trusted agent” with regard to the MSEL/PROFLOW and as such must protect the data as privileged information, guarding against its disclosure to organization members, or players, actually responding to the exercise challenge.

9. Virtual News Network considerations

Virtual News Network (VNN) accomplished many successes during T2. Future exercises could benefit from some changes and augmentation of VNN operations. The T2 design process can improve to ensure VNN announcements and interviews faithfully correlate with exercise play. Another consideration is the cost of VNN play. Though many recommended that VNN operations continue around the clock, planners must weigh the value of extended VNN play against cost. To add further realism to a simulation, VNN could record and play back its broadcasts during off hours, or provide a 24-hour Web-based news source such as www.VNN.com. Future VNN efforts should be targeted at aggressive news gathering that actively seeks sources for stories.

10. Exercise security considerations

Awareness of exercise participant safety and security concerns need to permeate exercise planning and operation. The possibility that sensitive information or closely-held responder procedures might fall into the wrong hands needs to be minimized. Enhanced physical, as well as electronic, security in the venues and the master control sites should be priorities in future events.

11. Exercise coordination and venue design team empowerment

Exercise venue design teams could be empowered to make recommendations regarding equipment and training preparedness needs, based upon their subject matter expertise and insight into existing domestic preparedness programs. The smaller, building-block events leading up to the FSE can be used as tools to enable or increase FSE success. These challenges also present continuous opportunities to identify State and local training, procedural, equipment, and preparedness shortcomings prior to the FSE. Closer linkage to statewide, multi-year Homeland Security strategies under DHS/ODP grant programs will improve the ability to identify needs.

IX. CONCLUSIONS

Following on the success of TOPOFF 2000, TOPOFF 2 (T2) was truly a groundbreaking exercise. It was particularly noteworthy as the first national exercise conducted since the Department of Homeland Security (DHS) was established. As a result, it provided a tremendous learning experience both for DHS and for the Federal agencies that will now be working with DHS during the response to domestic incidents. In addition, the experience in Washington and Illinois provided important lessons regarding Federal, State, and local (FSL) integration. These lessons are valuable to other states and localities as they work to train, exercise, and improve their own response capabilities.

A. T2 involved the play of new agencies and entities within DHS (e.g., the Transportation Security Agency, the Principle Federal Official, and the Crisis Action Team)

- The Principle Federal Official (PFO) concept was tested in both exercise venues. While this position has the potential to assist greatly with the coordination of federal activities across the spectrum of the response, T2 results also indicated that the roles and responsibilities of the PFO need to be clarified with respect to those of the Federal Bureau of Investigation Special Agent in Charge, the Federal Emergency Management Agency (FEMA) Regional Director, and the Federal Coordinating Officer, and potentially others. In addition, the PFO requires an emergency support team with the flexibility and expertise to provide support across the full range of homeland security operations. Other areas requiring clarification include transportation and medical assets now administered through DHS.

B. T2 represented the first time (real or exercise) in which the Homeland Security Advisory System Threat Condition was raised to Red

- This was a beneficial experiment in that the Secretary of DHS both raised selected areas of the country and then the whole country to Red. In addition, local jurisdictions raised their own threat conditions to Red;
- T2 revealed considerable confusion about the notification process and notification channels from the Federal Government to state and local governments. Local efforts to raise their own threat conditions produced confusion elsewhere in the country as to whether the statuses of the local conditions were DHS-driven actions. There was also confusion at all levels of government about what actions should be taken at Red, particularly in the case of selected locations; and
- Finally, although it was not fully explored during the exercise, concern was raised about the costs of being at Threat Condition Red—particularly in the absence of specific threat information.

C. T2 involved an extraordinary sequence of two Stafford Act Declarations wrapped around a Public Health Emergency Declaration by the Secretary of Health and Human Services

- The Presidential declarations were for a major disaster in the Washington venue and an emergency in the Illinois venue. These two declarations illustrated some of the subtleties of the Stafford Act that may not have been fully appreciated before the exercise; for instance, a bioterrorism attack does not clearly fit the existing definition of *disaster* as defined by the Act. ; and
- The Secretary of Department of Health and Human Services (HHS), acting on authorities through the Public Health Service Act and in consultation with the region, declared a Public Health Emergency. This permitted HHS to authorize the use of federal assets (with costs covered by HHS). It appeared to lead to some confusion about where authority to deploy certain assets really lay, with HHS or DHS.

D. Planning and development of the National Incident Management System should take advantage of the T2 experience

- This comment from the TOPOFF 2000 report bears repeating: “Multiple direction and control nodes, numerous liaisons, and an increasing number of response teams complicated coordination, communications, and unity of effort.” If anything, T2 may have been characterized by even more teams and communication nodes;
- Communication and coordination issues drove the course and outcome of critical public policy decisions from the elevation of the Threat Condition, to the various disaster/emergency declarations, the determination of exclusion zones, and the re-opening of transportation systems. To the extent that there were problems in these areas, communication issues were likely the primary cause; and
- T2 showed that how people believe communications and coordination are supposed to work is often not how they work in practice. What may appear to be clearly defined processes—such as requesting the Strategic National Stockpile—in practice become much more difficult. The National Incident Management System process needs to leverage the T2 experience.

E. T2 represented one of the largest hospital mass casualty exercises ever conducted, as 64 hospitals in the greater Chicago area participated in response to the bioterrorism attacks, and 123 hospitals either received faxed patients or participated in the communications of the exercise

- As such, T2 represented a significant experiment in communications and coordination for the public health and medical communities. In particular, the massive amounts of communication required to track resource status (e.g., beds, specialized spaces, medical equipment) taxed hospital staffs;
- T2 did not last long enough to fully explore the impacts of mass casualties due to bioterrorism on the medical system. Much less than half of the infected population was visible to the medical system at the conclusion of the exercise. This remains an area to explore in future exercises; and
- While there were a number of attempts to estimate the potential scope of the outbreak, the focus of most activities appeared to be on the cases that were presented to the health care

system. It should be noted that HHS was working actively as the week went on to identify the resources that would be required to deal with the infected population.

F. In the Illinois venue, T2 play involved an extensive Strategic National Stockpile request and distribution component

- Although the actual distribution process appeared to go quite well, there was some confusion over the procedures and processes for requesting and receiving the stockpile. The SNS Operations Center coordinated the stockpile deployment with the Centers for Disease Control and Prevention (CDC) and the FEMA EP&R Director; however, there is no data to indicate that senior-level consultation occurred between DHS and HHS. In addition different jurisdictions in Illinois took different routes (for example, through DHS FEMA and the CDC) to request the SNS; and
- The jurisdictions in the Illinois venue were forced to confront important decisions about how the stockpile (and local assets) would be divided and which population groups would be the first to receive prophylaxis. The discussions and decision-making involved, as well as the challenges of coordinating public information, provide valuable lessons to any metropolitan area.

G. The Department of Homeland Security should consider integrating the existing response policies and plans into the National Response Plan

- States are familiar with and have built their response plans to interact with federal assets using similar agency and department structures and language;
- Federal agencies are satisfied with the language, authorities, and relationships outlined in existing plans such as the Federal Radiological Emergency Response Plan and the National Oil and Hazardous Substances Pollution Contingency Plan; and
- As the National Response Plan continues to be developed, the surrounding issues merit consideration—particularly where existing plans are considered effective for emergency response.

H. T2 involved more intense and sustained top official play than occurred during TOPOFF 2000

- Of particular note was the play of DHS (which had been in existence for only a little more than ten weeks prior to the exercise), including the Secretary and other senior civilians; and
- HHS operated the Secretary's Command Center, non-stop, throughout the exercise with extensive play at the Assistant Secretary and Operating Division Director level. The Secretary was actively involved in T2 play, and since the Illinois venue involved substantial public health and medical play, the active participation of HHS was critical to the success of the exercise.
- In both the Washington and Illinois venues, the offices of the mayors, county executives, and governors were well represented throughout the exercise by either the elected officials themselves or high-level policy-makers in respective administrations. In particular, the Mayor of Seattle participated substantially in the FSE, providing local top

leadership that greatly contributed to the realism of play and to a greater appreciation of the local challenges and perspectives in a national WMD attack.

I. T2 represents a foundational experience to guide the future development of the TOPOFF exercise series

- Because of the intense data collection process and the effort to make T2 findings traceable through a detailed reconstruction of the exercise events, T2 now represents a baseline upon which subsequent TOPOFF exercises can build and to which they can be rigorously compared. In addition, continued analyses of T2 data can be employed to help guide the design of the National Exercise Program.
- T2 demonstrated the value of the international, private sector, and non-profit perspectives and roles in any response to WMD terrorism. Future exercises will, no doubt, expand on these elements by broadening the participation of these sectors.
- The use of an opposing force (OPFOR), or red team, during T2 provided ground rules for the involvement of a simulated active enemy threat in future exercises. This play should also be expanded in future exercises, as it represents one of the fundamentally different challenges responders face in a terrorist WMD disaster relative to any natural or conventional disaster; and
- The success of the VNN, and widespread participant feedback regarding the desire for additional challenges in the area of public information, suggest that future exercises should include a more aggressive mock-media element, with a more aggressive news gathering function.

X. GLOSSARY OF ABBREVIATIONS AND ACRONYMS

A

AAC	After Action Conference
AAR	After Action Report
ADLE	Advanced Distance Learning Exercise
ALS	Advanced Life Support
AMS	Aerial Measuring System
AMTRAK	National Railroad Passenger Corporation
ARAC	Atmospheric Release Advisory Capability
ARC	American Red Cross
ASPHEP	Assistant Secretary Public Health Emergency Preparedness (HHS)
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives

B

BEN	Business Emergency Network
BDC	Bomb Data Center (FBI)
BLS	Basic Life support
BTS	Border and Transportation Security (DHS)

C

CA	California
CAN	Canada
CAT	Crisis Action Team
CBP	Customs and Border Protection (DHS)
CBR	Chemical, Biological, Radiological
CBRN	Chemical, Biological, Radiological, Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CCU	Hospital Critical Care Unit
CDC	Centers for Disease Control and Prevention
CDC EIS	CDC Epidemic Intelligence Service
CDPH	Chicago Department of Public Health
CDT	Central Daylight Time

CEO	Chief Executive Officer
CFR	Code of Federal Regulation
CIRG	Critical Incident Response Group (FBI)
CMC	Crisis Management Center
CMG	Consequence Management Group
CMT	Crisis Management Team (Kane County, IL)
CO	Colorado
COG	Continuity of Government
CONPLAN	United States Government Interagency Domestic Terrorism Concept of Operations Plan
COOP	Continuity of Operations Plans
CPX	Command Post Exercise
CST	Civil Support Team (National Guard WMD – CST)
CT/NP-ESG	Counter-Terrorism and National Preparedness Exercise Sub-Group
CYBEREX	Cyber Exercise

D

DC	District of Columbia
D-Day	D-Day (-/+) (T2 Full Scale Exercise Start Date)
DEST	Domestic Emergency Support Team
DFO	Disaster Field Office (FEMA)
DHS	Department of Homeland Security
DHS CAT	DHS Crisis Action Team
DHS CBP	DHS Bureau of Customs and Border Protection
DHS EP&R	DHS Emergency Preparedness and Response
DHS ICE	DHS Immigration and Customs Enforcement
DHS/ODP	DHS Office for Domestic Preparedness
DHS/OER	DHS Office of Emergency Response
DHS/TSA	DHS Transportation Security Agency
DMAT	Disaster Medical Assistance Team
DMORT	Disaster Mortuary Operational Response Team
DOD	Department of Defense
DOE	Department of Energy
DOE RAP	DOE Radiological Assistance Program

DOE AMS	DOE Aerial Measuring System
DOE ARAC	DOE Atmospheric Release Advisory Capability
DOE NNSA	DOE National Nuclear Security Administration
DOH	Department of Health
DOH/DRP	“Washington State Department of Health, Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack”
DOI	Department of Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOS S/CT	DOS Office of the Coordinator for Counterterrorism
DOT	Department of Transportation
DOT CMC	DOT Crisis Management Center
DPH	Department of Public Health
DSHL	Deputy State Health Liaison (Washington State)
DTRA	Defense Threat Reduction Agency
DTRA HPAC	DTRA Hazard Prediction and Assessment Capability

E

ED	Emergency Department
EDT	Eastern Daylight Time
EIS	CDC Epidemic Intelligence Service
EMnet	Emergency Management Network
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
EPA RRC	EPA Regional Response Center
EPA RERT	EPA Radiological Emergency Response Team
EPI	Emergency Public Information
EP&R	Emergency Preparedness and Response (DHS)
EPR	Emergency Preparedness and Response (DHS)
ER	Hospital Emergency Room
ERT	Emergency Response Team

ERT	Evidence Response Team (FBI)
ESF	Emergency Support Function
ESMARN	Emergency Services Mutual Aid Radio Network
ESP	Extranet Secure Portals
EST	FEMA Emergency Support Team
EXPLAN	Exercise Plan

F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBI BDC	FBI Bomb Data Center
FBI CIRG	FBI Critical Incident Response Group
FBI ERT	FBI Evidence Response Team
FBI HMRU	FBI Hazardous Materials Response Unit
FBI HRT	FBI Hostage Rescue Team
FBI SAC	FBI Special-Agent in Charge
FCO	Federal Coordinating Officer
FDA	Food and Drug Administration
FE	Functional Exercise
FEMA	Federal Emergency Management Agency
FEMA EST	FEMA Emergency Support Team
FEMA NIEOC	FEMA National Interagency Emergency Operations Center
FOUO	For Official Use Only
FPS	Federal Protective Service
FRA	Federal Railroad Administration
FRERP	Federal Radiological Emergency Response Plan
FRMAC	Federal Radiological Monitoring and Assessment Center
FRP	Federal Response Plan
FSE	Full Scale Exercise
FSL	Federal, State, & Local

G

GIS	Geographic Information System
GLODO	Group for the Liberation of Orangeland & the Destruction of Others

GMT Greenwich Mean Time
GSA General Services Administration

H

HAN Health Alert Network
HAM Amateur Radio Operator
HAZMAT Hazardous Material
HDER DOE/DOJ Homeland Defense Equipment Reuse program
HHS Health and Human Services
HHS ASPHEP HHS Assistant Secretary Public Health Emergency Preparedness HHS
HHS SERT HHS Secretary's Emergency Response Team
HHS SCC HHS Secretary's Command Center
HIPAA The Health Insurance Portability and Accountability Act
HMRU Hazardous Materials Response Unit (FBI)
HPAC Hazardous Predicting Assessment Capabilities
HQ Headquarters
HRT Hostage Rescue Team (FBI)
HSAS Homeland Security Advisory System
HSC Homeland Security Council
HSCenter Homeland Security Center (DHS)
HSPD-3 Homeland Security Presidential Directive-3,
"Homeland Security Advisory System"
HSPD-5 Homeland Security Presidential Directive-5,
"Management of Domestic Incidents"
HUD Department of Housing and Urban Development

I

I-5/I-90 Interstate Highway 5/ Interstate Highway 90
IA Interagency
IAIP Information Analysis and Infrastructure Protection (DHS)
IC Incident Commander
ICE Immigration and Customs Enforcement (DHS)
ICS Incident Command System
ICU Hospital Intensive Care Unit

IDPH	Illinois Department of Public Health
IEMA	Illinois Emergency Management Agency
IL	Illinois
ILCS	Illinois Compiled Statutes
IL DOT	Illinois Department of Transportation
IMERT	Illinois Mobile Emergency Response Team
ING	Illinois National Guard
IOHNO	Illinois Operational Headquarters and Notification Office
IPS	Illinois Pharmaceutical Stockpile
ISO	Incident Safety Officer
IST	Incident Support Team
IUSAR	Illinois Urban Search and Rescue Team
IV	Intravenous

J

JIC	Joint Information Center
JOC	Joint Operations Center
JTF	Joint Task Force (DOS)
JTTF	Joint Terrorism Task Force

K

KC	King County, (Washington)
KCC	King County Charter, (Washington)
KCOEM	King County Office of Emergency Management
KLERN	Kane Local Emergency Radio Network (Kane County, IL)

L

LFA	Lead Federal Agency
LINC	Local Integration to access NARAC with Cities program
LNO	Liaison Officer
LSG	Large Scale Game

M

MALS	Mobil Analytical Laboratory System
------	------------------------------------

MCC	T2 Exercise Master Control Cell
MCFR	Montgomery County (Maryland) Fire Rescue
MCHC	Metropolitan Chicago Healthcare Council
MD	Medical Doctor
MERRT	Medical Emergency Radiological Response Team (Veterans Affairs)
MERS	Mobile Emergency Response System (National Guard)
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSEL	Master Scenario Events List

N

NARAC	National Atmospheric Release Advisory Capability
NASA	National Aeronautics and Space Administration
NCP	National Oil & Hazardous Substances Pollution Contingency Plan
NCR	National Capital Region
NCR FE	National Capital Region, Functional Exercise
NDMS	National Disaster Medical System
NIEOC	National Interagency Emergency Operations Center
NIMS	National Incident Management System
NNSA	National Nuclear Security Administration
NOAA	National Oceanic and Atmospheric Administration
NRC	Nuclear Regulatory Commission
NRP	National Response Plan
NSC	National Security Council
NSC PCC	National Security Council, Policy Coordinating Committee
NSC PCC (CT/NP-ESG)	National Security Council, Policy Coordinating Committee, Counter Terrorism and National Preparedness Exercise Sub-Group
NWS	National Weather service
NY	New York

O

ODP	Office for Domestic Preparedness
OEM	Office of Emergency Management
OER	Office of Emergency Response (DHS)

ONCRC	Office of National Capital Region Coordination
OPFOR	Opposing Force – Opposition Force
OSHA	Occupational Safety and Health Administration

P

PA	Public Address system
PAG	Protective Action Guidelines
PCC	Policy Coordinating Committee
PCR	Polymerase Chain Reaction
PDD-39	Presidential Decision Directive–39 <i>“U.S. Policy on Combating Terrorism”</i>
PDT	Pacific Daylight Time
PFD	Phoenix Fire Department
PFO	Principle Federal Official
PHSKC	Public Health Seattle/King County
PIO	Public Information Officer
POC	Point-of-Contact
POD Hospital	Illinois Disaster POD Hospital. Term used by the IDPH disaster plan for hospitals designated to consolidate and coordinate regional hospital medical information for further transmission to IOHNO.
PPE	Personal Protective Equipment
PROFLOW	Procedural Flow Synopsis
PRO-NET	Professional Reporting Network (DuPage County)

Q

R

RAP	Radiological Assistance Program
RCW	Revised Code of Washington
RD	Region Director (FEMA)
RDD	Radiological Dispersion Device
REOC	Regional Emergency Operations Center
RERT	Radiological Emergency Response Team (EPA)
RN	Registered Nurse
ROC	Regional Operations Center (FEMA)

RMAC	Radiation Monitoring and Assessment Center (Washington State)
RRC	Regional Response Center (EPA)

S

SAC	Special-Agent in Charge (FBI)
SAMHSA	The Substance Abuse and Mental Health Services Administration
SARS	Severe Acute Respiratory Syndrome
SCC	Secretary's Command Center (HHS)
SDS	Same Day Surgery
SeaTac	Seattle-Tacoma International Airport
SEO	Senior Energy Official
SEOC	State of Illinois Emergency Operations Center
SERT	Secretary's Emergency Response Team (HHS)
SFD	Seattle Fire Department
SHL	State Health Liaison (Washington State)
SIOC	Strategic Information and Operations Center
SIRT	The State Interagency Response Team (Illinois)
SME	Subject Matter Expert
SNS	Strategic National Stockpile
SNSOC	Strategic National Stockpile Operations Center
SODO	South of Downtown district of Seattle
SPD	Seattle Police Department
S&T	Science & Technology (DHS)
STB	Surface Transportation Board

T

TOPOFF	TOP OFFICIALS EXERCISE SERIES
"TOPS"	TOPOFF Pulmonary Syndrome
T2	TOPOFF 2
T2 FSE	TOPOFF 2 Full Scale Exercise
T2 LSG	TOPOFF 2 Large Scale Game
TFR	Temporary Flight Restrictions
TOPS syndrome	TOPOFF Pulmonary Syndrome
TSA	Transportation Security Agency

TTX	Table Top Exercise
TV	Television
TX	Texas

U

US	United States
USAR	Urban Search and Rescue
USCG	United States Coast Guard
USDA	United States Department of Agriculture
USGS	United States Geological Survey
UT	Universal Time
UTC	Coordinated Universal Time

V

VA	Department of Veterans Affairs
VA MERRT	VA Medical Emergency Radiological Response Team
VCC	T2 Exercise Venue Control Cell
VMI	Vendor Managed Inventory
VNN	Virtual News Network
VTC	Video Teleconference

W

WA	Washington
WA DOH	Washington State Department of Health
WA DOT	Washington Department of Transportation
WDOT	Washington Department of Transportation
WHO	World Health Organization
WMD	Weapons of Mass Destruction

X-Y-Z

TOP OFFICIALS (TOPOFF) EXERCISE SERIES:

TOPOFF 2 (T2) After Action Report ANNEX A



September 30, 2003

Information contained in this document is intended for the exclusive use of T2 Exercise Series participants. Material may not be reproduced, copied, or furnished to non-exercise personnel without written approval from the Exercise Directors.

This page intentionally left blank

TOPOFF 2 Electronic Reconstruction Product

NOTE TO USERS:

Background: This file provides an electronic, searchable reference of significant domestic (United States) events and decisions that occurred in the TOPOFF 2 (T2) Full Scale Exercise (FSE) between May 12-May16, 2003. The events in this reconstruction took place in 3 venues: the State of Washington (WA), State of Illinois (IL), and Washington DC (referred to as the "Interagency," and abbreviated as "IA"). It was developed through the reconstruction process detailed in the T2 After Action Report (AAR) and distilled from more than 20,000 lines of raw data entered directly from data collector logs, controller records, participant and agency logs, situation reports, and emails. This file is NOT data. It reflects analysis and follow-up work by analysts to deconflict data within and between venues. Its purpose is as a reference to participating and non-participating entities to provide them a sense of the significant events, activities, and decisions that were faced by the national response community in response to the events in the T2 FSE scenario- a perspective no single agency could have on its own. This does not provide a detailed account of any particular agency's actions.

Additional Notes:

Note that all times reflect Eastern Daylight Time (EDT), which was the official exercise time. Original times have been converted in order to provide an integrated and time-synchronized perspective.

Note that the "Source" Column refers to the organization or organizations which submitted data to support the event/activity/decision listed. There may have been additional organizations that documented any given event/activity/decision.

An Acronym list is provided for the entire Reconstruction as well as for references specific to each venue.

All events/activities/decisions are associated with the venue of their occurrence in the "Venue" column.

The Reconstruction ends with the last event/activity of significance in the FSE at 204 hours on 15 May.

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	12-May-03	14:00	INJECT: The DEST departs Andrews Air Force Base in response to a credible threat against the Columbia Generating Station in Richland, WA. (MSEL # 3042)	Event was notional so time is notional		DOT CMC
IA	12-May-03	14:58	At 11:58 Virtual News Network (VNN) begins coverage of an explosion in the South of Downtown (SODO) District in Seattle, WA.	Time ranges from 11:58 to 12:03 PDT (14:58 to 15:03 EDT). Time chosen was from WA VCC Official time and MSEL Team log.	MSEL; TopOff Log; Data Collector Logs; Data Collector Log; Analyst Log; Data Collector Logs; Data Collector Log	WA State EOC; KC EOC; RDD site; VNN; FEMA Region X ROC; KC RJIC
IL	12-May-03	15:00	IL SEOC reports that there has been a reported explosion in Seattle. At this point, it is not certain what the cause of the explosion was. Agency liaisons to be contacted to report to the IL SEOC. Advised to notify IEMA Director.		SEOC Event Log	IL State EOC
WA	12-May-03	15:00	Upon watching the initial VNN report, FEMA Region X Regional Operations Center (ROC) Director notified Emergency Support Function (ESF) lead agencies and requested they send liaisons to staff the ROC (corresponds to MSEL # 2052).	Time taken was from data collector at the IOF, other times were recorded at 14:02 and 13:10 PDT (17:02 and 16:10 EDT) by the MSEL team from unknown sources. Action initiated from VNN report. In fact many ESF representatives actually came to the EOC that morning, before STARTEX.	Data Collector Log	FEMA IOF
IA	12-May-03	15:00	SNS Operations Center activated		CAT team operations report	DHS CAT
IL	12-May-03	15:03	Chicago OEMC elevates local alert level from Yellow to Orange		Data Collector Log	Chicago EOC
WA	12-May-03	15:03	Upon watching the initial VNN report, Seattle EOC notifies the King County EOC of an explosion in the SODO District of the city (corresponds to MSEL # 2023).	Time was taken from first report to KC EOC by Seattle EOC at 12:03 PST (15:03 PDT). Other times are 12:04 PDT (15:04 EDT) from the MSEL spreadsheet, 12:10 PDT (15:10 EDT) from the same data collector reporting 12:03 PDT (15:03 EDT), and 12:28 PDT (15:28 EDT) from the MSEL spreadsheet.	MSEL; Data Collector Logs	Seattle EOC; KC EOC; WA State EOC
WA	12-May-03	15:04	Based on VNN report, Seattle FBI Field Office Operations Coordinator notifies SIOC (corresponds to MSEL # 2017)	Time was chosen from data collector log at WA State EOC. SIOC OPS Coordinator Log records notification at the same time	Data Collector Log	WA State EOC
IL	12-May-03	15:05	IL SEOC activated		Data Collector Log	IL State EOC
WA	12-May-03	15:05	After watching the initial VNN report, the Seattle EOC notifies Washington State Ferry (WSF) EOC of the explosion in the SODO District of the city. They acknowledge that they are aware of the problem and have activated their EOC (corresponds to MSEL # 2015).	Time used was obtained from WSF Lead Controller at WSF EOC. Other times were 12:06 PDT (15:06 EDT) from a Seattle EOC DC and 12:10 PDT (15:10 EDT) from the MSEL Team (unknown source).	MSEL Team	
WA	12-May-03	15:08	STARTEX: At 12:08 an explosion occurs at the intersection of 8th Ave S and South Hanford Street (MSEL # 2005).	STARTEX was delayed by VCC Director for 10 minutes due to placement of victims. Time taken was from WA VCC Official time, analyst on site at RDD and MSEL Team log. Other reported times ranged from 12:08 to 12:10 PDT (15:08 to 15:10 EDT).	MSEL Team; Analyst Log	RDD site
WA	12-May-03	15:09	INJECT: Seattle Police and Fire dispatch simulate getting 911 calls. Seattle Police notifies nearby units to respond and investigate. Based on the simulated call volume and call descriptions, Seattle Fire sends an appropriate response (MSEL # 2006).	Police and Fire dispatch were part of the exercise SIMCELL. The initial dispatches that were sent out were done as injects not as reactions to 911 calls. There were no simulated 911 calls.	MSEL	MSEL
WA	12-May-03	15:10	Seattle EOC Director begins the EOC's notification chains (corresponds to MSEL # 2014).	Time taken from Seattle EOC DC log.	Data Collector Log	Seattle EOC
WA	12-May-03	15:10	First responding units arrive on scene, including SFD Engine #2, ambulance and 9 SPD patrol cars. All of these units initially still alarmed or on-viewed (self-dispatched) based on hearing the explosion (corresponds to MSEL # 2010).	Information taken from several DC log entries that occur between 12:08 and 12:13 PDT (15:08 and 15:13 EDT).	Data Collector Logs	RDD site; KC EOC; Harborview EOC
WA	12-May-03	15:10	Public Health-Seattle&King County (PHSKC) EOC activates in response to the notification by the Seattle EOC of the explosion (corresponds to MSEL # 2018).	No data points suggest that PHSKC EOC was notified by Hospital Control as was called for in the MSEL. At 12:10 PDT (15:10 EDT) Seattle EOC notified PHSKC EOC. At 12:25 PDT (15:25 EDT) the incident commander notified PHSKC EOC as well.	Data Collector Log	Seattle EOC
WA	12-May-03	15:10	WA SEOC notified of the explosion and activated to Phase III (corresponds to MSEL # 2025)	Time notes when WA SEOC was notified, not by whom (MSEL called for the WA SEOC to be notified by the Seattle EOC). Time as taken from data collector at WA SEOC. Other times collected by the MSEL team were 12:11 and 12:30 PDT (15:11 and 15:30 EDT).	Data Collector Log; MSEL Team	WA State EOC
WA	12-May-03	15:10	FEMA Region X informed that the WA SEOC is activated (corresponds to MSEL # 2039)	Time taken was from DC in WA SEOC. WA SEOC made call based on VNN report, not actual detonation. Other times reported were 12:36 by the MSEL team and 12:00 by the FEMA VCC Rep.	EOC Supervisor Log; MSEL Team	WA State EOC
IA	12-May-03	15:11	Message sent by HHS Secretary's Command Center (SCC) to COOP Notification, through Roam Secure Alert Network: A large explosion in the SODO District of Seattle, WA, unknown source of explosion, unknown injuries.		Agency Log	DHS/HS Center
WA	12-May-03	15:12	SFD announced that victims who can walk should slowly approach Engine #2; those who need help are instructed to stay where they are	Announcement started at 12:12 PDT (15:12 EDT) and was continuous to at least 12:18 PDT (15:18 EDT).	Data Collector Log	RDD site
WA	12-May-03	15:12	Seattle EOC activated to Phase III operations		Seattle EOC Log	Seattle EOC
WA	12-May-03	15:12	Washington State Emergency Management Division (WA EMD) Director calls the WA SEOC and orders a Phase III (Full Operations) activation.		Data Collector Log	WA State EOC
IA	12-May-03	15:12	EPA Region 10 On Scene Coordinator deployed to incident site		Data Collector Log	EPS Aux. Ops Ctr

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	12-May-03	15:14	CPD notified the following departments and agencies about the explosion in Seattle:		Data Collector Log	Chicago EOC
IL	12-May-03	15:15	Chicago EOC Activated		Data Collector Log	Springfield IL EOC
IA	12-May-03	15:15	Report to SIOC that the FBI SAC has been notified, the ERT and SWAT recalled, and an on-scene commander dispatched		OPS Coordinator Component Log	SIOC
IA	12-May-03	15:20	FEMA EOC receives call from FEMA Region X ROC reporting a bomb blast in Seattle		OPS Coordinator Component Log	FEMA EOC
WA	12-May-03	15:21	Based on the report from the City of Seattle Emergency Operation Center regarding a large explosion in the vicinity of 2700 Airport Way, the King County Emergency Operation Center (EOC) has been activated at Level III. The cause of explosion is unknown; no other details are available at this time.		Press Release	KC IC
WA	12-May-03	15:22	INJECT: Seattle Fire Department Unit 77 (HAZMAT) simulated responding from Station 2 (SFD HQ). This would have brought them through the plume, so as they were responding controllers informed players that there radiation pagers alarmed (MSEL # 2013).	Time came from Fire Alarm Center's call log. Unit 77 (HAZMAT) immediately called in when there radiation pager alarmed. Data Collector logs had the time at 12:29 PDT (15:29 EDT) from the KC EOC, 12:22 PDT (15:22) EDT from radio traffic overheard at the RDD Site, and 12:21 PDT (15:21 EDT) from the SFD FAC.	Data Collector Logs	KC EOC; RDD Site; SFD FAC
WA	12-May-03	15:25	A triage station is being set up near Ladder 7 and multi casualty units, 150 yds south of bomb site	Time taken was from RDD Site Technical Decon Controller. Only clear data point about Triage.	Data Collector Log	RDD site
IA	12-May-03	15:25	SIOC receives report from DHS that radiation was detected in Seattle		Data Collector Log	FBI SIOC
IA	12-May-03	15:25	VNN update: unconfirmed report of detection of radiation		Data Collector Log	CDC EOC Atlanta
WA	12-May-03	15:29	At 1230 the city of Seattle lead PIO authorizes a press release acknowledging the activation of the EOC and response of the city's first responders to an explosion. Text: FOR IMMEDIATE RELEASE 1230, 12 May 2003 SUBJECT: Seattle EOC Activated FOR MORE INFORMATION CONTACT: City of Seattle EOC Media Line: (206) 233-5072 http://www.seattle.gov City of Seattle Activates Emergency Operations Center to respond to emergency south of downtown Seattle The Seattle Police Chief activated the City of Seattle's emergency operations center just past noon today in response to an explosion south of downtown Seattle. Police and Fire personnel are on scene to determine the nature of the blast. Citizens are urged to avoid the area within a mile of Airport Way S. and S. Hinds Street. The Seattle Mayor is being briefed and will address the public as soon as possible.		Press Release	Seattle EOC
WA	12-May-03	15:30	Washington State Top Officials in the WA SEOC Policy Room alert the Washington State National Guard WMD Civil Support Team to go on standby and prepare to deploy in support of the City of Seattle.		EOC Supervisor Log	WA State EOC
WA	12-May-03	15:30	FBI SAC notified that radiation was detected at the incident site. The SAC requested the DEST and HMRU and requested that the SIOC be notified (corresponds to MSEL # 3045).	Time taken was from FBI SAC Log, but where the notification came from is not noted (MSEL called for notification to come from the Seattle EOC). Other time 12:35 PDT (15:35 EDT) from MSEL Team - source unknown.	SAC Log Data; MSEL Team	FBI WA Field Office
WA	12-May-03	15:32	The Washington State Ferry EOC locked down all ferried and shut down service (corresponds to MSEL # 2026).	Time was taken from WA SEOC data collector observing WSP. Earliest time reported that Ferries were shut down. This entry was recorded later, but specifically mentions 12:32 PDT (15:32 EDT) as shut down time. Other entries merely not time call was received or are time update was given, not time ferries were shut down. Other reported times - 13:25 PDT (16:25 EDT) from a DC at the KC EOC, MSEL team times 12:34 PDT (15:34 EDT) reported to the MSEL team from an unknown source, and 12:40 PDT (15:40 EDT) reported to the MSEL team from the WSF Lead Controller.	Data Collector Log; MSEL Team	KC EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	15:32	INJECT: The detection of cesium was injected to the Incident Commander. The MSEL item represented was the time that the FBI thought they would detect it. The IC controller saw the time come and pass and injected this information without permission from the VCC. Other times recorded for this occurring were 13:30 and 14:15, captured by MSEL team, source unknown (MSEL # 2031).	The detection of cesium was injected to the Incident Commander. The MSEL item represented was the time that the FBI thought they would detect it. The IC controller saw the time come and pass and injected this information without permission from the VCC. Other times recorded for this occurring were 13:30 and 14:15 PDT (16:30 and 17:15 EDT), captured by MSEL team, source unknown.	MSEL Team	WA VCC
IL	12-May-03	15:33	DuPage County EOC notified IL SEOC of explosion in Seattle; moving to initiate EMNet (satellite based point-to-point secure communications network of all EOC's)		Data collector Log	DuPage Co. EOC
IL	12-May-03	15:35	IEMA notified CCSEMA about an explosion in Seattle with possible detection of radiation. Also notified that IEMA has opened its EOC		Message & Event Log	CCSEMA
IA	12-May-03	15:35	INJECT: HHS SCC notifies HHS SERT of the incident in Seattle (MSEL # 3106)		Data Collector Log	FDA EOC
IL	12-May-03	15:36	Chicago EOC holds Radioactive Dispersal Devices (RDDs) consequence briefing		Data Collector Log	Chicago EOC
WA	12-May-03	15:36	This is the time in the MSEL that SFD HazMat and/or SPD Arson/Bomb Squad was to receive radiation alerts on their monitoring devices. There are no clear observations from data collectors. Many report HAZMAT or ABS showing up on scene and some of their activities, but there are no clear descriptions of them confirming the radiation readings (corresponds to MSEL # 2024).		MSEL Team	WA VCC
IA	12-May-03	15:37	Message sent by HHS SCC to COOP Notification, through Roam Secure Alert Network: Radiation has been detected in the explosion in the SODO District of Seattle. Unknown radiological type and level.		Agency Log	DHS/HHS Center
WA	12-May-03	15:38	WA EMD Director approves the first press release acknowledging an event in the City of Seattle and describing WA State's current response to the situation. Press Release: CAMP MURRAY, WA- The State Emergency Operations Center (EOC) at Camp Murray was activated at 12:10 p.m. today in response to an explosion in the south. The WA Governor has been informed of the incident. Representatives from the state departments of Military (Emergency Management); Health; Transportation; Ecology; Agriculture; and the State Patrol as well as the American Red Cross are reporting to the State EOC.	Press release was from DC notes, may not be exact wording.	Data Collector Log	WA State EOC
WA	12-May-03	15:40	Decontamination area being established at incident site		Data Collector Log	RDD site
WA	12-May-03	15:40	WA Governor has been informed of the incident.		Press Release	WA State EOC
IA	12-May-03	15:40	CDC EOC Emergency Response Coordinator prepares message to notify CDC's centers, institutes & offices of the radiological incident in Seattle		Data Collector Log	CDC EOC Atlanta
IA	12-May-03	15:40	FDA receives phone call from HHS SCC confirming radiation of unknown source in Seattle		Data Collector Log	FDA, EOC Rockville, MD
WA	12-May-03	15:41	King County EOC posts notification that security level is RED		Data Collector Log	KC EOC
IL	12-May-03	15:42	Chicago EOC notified BOMA, Sears, Aon Center, Hancock Buildings regarding potential terrorist threat		Data Collector Log	Chicago EOC
IA	12-May-03	15:42	FDA EOC activated		Data Collector Log	FDA, EOC Rockville, MD
IA	12-May-03	15:42	TSA desk at DOT CMC receives phone call from TSA representative at DHS confirming radiation in Seattle		Data Collector Log	DOT CMC
IA	12-May-03	15:44	VACO receives confirmation from DHS that radiation has been detected in Seattle		Data Collector Log	VA Central Office
IL	12-May-03	15:45	Chicago DPH reports HAN is looking for unusual disease clusters		Data Collector Log	Chicago DPH
IL	12-May-03	15:45	CPD feels that an attack by terrorist group "GLODO" is imminent; looking at nuclear targets. Chicago is at a "heightened alert" status, increasing awareness and vigilance at possible targets		SEOC Event Log	IL State EOC
IA	12-May-03	15:50	Reports coming in to HHS SCC from DHS about Pu 229, Ce 137, and Americium	While this did occur in the exercise, there is no way that the three radioactive components could have been identified this early in the exercise. HHS liaisons in WA discounted this information and it did not impact play.	Data Collector Log	HHS
WA	12-May-03	15:51	No chemical agents detected at the incident site	Actual time was between 12:51 and 12:59 PDT (15:51 and 15:59 EDT)	Data Collector Log	RDD site
IA	12-May-03	15:57	HHS sending SERT to Region X REOC		Data Collector Log	HHS
IA	12-May-03	15:57	Region X REOC officially activated		Data Collector Log	HHS
IA	12-May-03	15:57	HHS receives request from DHS to identify HHS assets that are available to deploy - need for brief to DHS Secretary		Data Collector Log	HHS

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	15:59	Hospital Control contacting all western WA hospitals with exception of Monroe County		Data Collector Log	Harborview EOC
WA	12-May-03	16:00	SFD advises SPD to set up a command post next to SFD command post for communication purposes. SPD Incident Commander directs arriving SPD personnel to set up perimeter		Data Collector Log	RDD site
WA	12-May-03	16:00	At 13:00 FEMA ROC Region X received notification that the Consequence Mangement Group at the JOC was stood up.		Data Collector Log	FEMA Region X ROC
IA	12-May-03	16:00	INJECT: DOS task force stands up in response to the explosion in Seattle (MSEL #4040)		Data Collector Log	HHS
IA	12-May-03	16:00	HHS SCC requests that CDC assemble team of SMEs that can potentially deploy to Seattle (corresponds to MSEL # 3111)		Data Collector Log	CDC EOC Atlanta
IL	12-May-03	16:01	Chicago EOC receives information from Chicago DPH that the HSAS has been elevated to RED. Chicago EOC holds at ORANGE until the information can be confirmed.		SEOC Event Log	IL State EOC
WA	12-May-03	16:02	FEMA Liaison reports that DHS Secretary dispatched a Forward Coordinating Team to assist the IC with determining resource needs.		Agency Log	WA State EOC
IA	12-May-03	16:02	DHS CAT Situation Report contains update that Greater Seattle is Threat Level RED		Situation Report	DHS-CAT
WA	12-May-03	16:03	SFD receives plume prediction from NARAC showing cloud moving N x NW (corresponds to MSEL # 2038)		MSEL	MSEL
WA	12-May-03	16:04	Law Team preparing Mayoral Proclamation of Civil Emergency Order Delegation of Authority. This was done in consultation with Mayor's general counsel		Agency Log	WA State EOC/Seattle EOC
IL	12-May-03	16:05	Chicago EOC contacted METRA, RTA, and CTA and briefed them on the situation; 'self-evacuation' locomotives back in town; decide to have CTA start "Rush Hour" earlier		Data Collector Log	Chicago EOC
WA	12-May-03	16:05	WA SEOC policy group asked staff to start on Governor's proclamation		EOC Supervisor Log	WA State EOC
WA	12-May-03	16:05	Air Space closure had been requested by IC and the WA SEOC, 5 mile radius and up to 1000 feet.		Agency Log	WA State EOC/Seattle EOC
IA	12-May-03	16:05	INJECT: FBI SIOC to Issue warning order to Crisis Medical Response Asset (corresponds to MSEL # 3673)		Data Collector Log	FBI SIOC
WA	12-May-03	16:06	Discussion at IC ensues about the NARAC model which leads to a recommendation to set up a 10 mile area where citizens should remain in doors. They can recommend this but there is not enough manpower to enforce it.		Data Collector Log	RDD site
WA	12-May-03	16:07	WA SEOC policy group asked staff to start on request for a presidential disaster declaration.		Data Collector Log	WA State EOC
IA	12-May-03	16:08	FAA reports to DOT Chief of Staff: Temporary Flight Restriction (TFR) has been issued for 30 mile radius around SEATAC airport air traffic control tower up to 20,000ft. All in bound traffic has been re-directed.		Data Collector Log	DOT CMC
WA	12-May-03	16:09	King County Executive instructs EOC staff to notify King County employees working in Seattle - tell them to shelter in place, but prepare for them to move		Data Collector Log	KC EOC
IL	12-May-03	16:10	Chicago EOC displaying Shelter-In-Place activities in Seattle; enacted vehicle parking prohibition near target areas in and around Chicago		Data Collector Log	Chicago EOC
IA	12-May-03	16:10	ICE Situation Room and ICE HQ Reporting Center activated.		Situation Report	DHS-CAT
IA	12-May-03	16:10	CDC NCEH convenes the Preliminary Assessment Team (PAT) to discuss the radiological event. The PAT agrees to activate the EOC - meaning response operations and associated support will center in the EOC. Additionally, the PAT discussed the potential radiological elements being reported--Plutonium 238/239, Cesium 137 and Americium. Most of the discussion focuses on the [exercise] "validity" of the elements reported to have been detected, given the detectors available on-scene at this time. CDC's lead for radiation indicated the only detection devices of a portable nature detect gamma emissions and therefore would not be able to detect these elements. CDC staff also alerted to be prepared to deploy to Seattle to support FRMAC		Data Collector Log	CDC EOC Atlanta
WA	12-May-03	16:14	Seattle EOC PIOs issue press releases in multi-languages		Agency Log	Seattle EOC
IA	12-May-03	16:15	EPA Auxiliary Operations Center receives report that radioactive materials have been detected in field at Seattle.		Data Collector Log	EPS Aux. Ops Ctr
IL	12-May-03	16:17	IDPH advises Chicago OEMC of change in alert status from Orange to Red; but not confirmed.		Data Collector Log	Chicago EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	16:17	Seattle DOT informed SPD of their recommendation to halt all traffic coming into downtown. They are developing a traffic plan.		Seattle EOC Log	Seattle EOC
IL	12-May-03	16:20	ARC of Greater Chicago received message that radiological activity detected in Seattle		Data Collector Log	ARC of Greater Chicago HQ
IA	12-May-03	16:20	FEMA EST receives request for 3 WMD task forces from ESF-9		Data Collector Log	FEMA EST
IA	12-May-03	16:20	NAWAS carried a message that the NCR had gone to RED.	The NCR had not gone to RED at this time	Data Collector Log	HHS
IA	12-May-03	16:26	HHS EOC inquiring as to source of Seattle weather data (e.g., wind direction). CDC radiation division is working on short / long term effects of the radiation release and will get information to hospitals on the isotopes.		Data Collector Log	HHS
IA	12-May-03	16:28	DHS HS Center received call from OSLGC Homeland Operations Center saying that the Federal Protection Services reported that the City of Seattle raised threat level to Red.		HSC OSLGC Incident Log	DHS/HS Center
WA	12-May-03	16:29	Update on WA DOT Road Closures: I-5 at I-405 north bound (Tukwilla) at I-5 at I-405 soundbound (Lynnwood), thus I-5 is closed down. I-90 and SR 520 are closed west bound into the City of Seattle, and the west bound lanes have been opened to Emergency routes east bound from the city of Seattle. Washington State Ferry EOC has shut down all routes and Ferry operations		IAP Section Activity Log	WA State EOC
WA	12-May-03	16:34	SPD SWAT and SPD EOD agree to link up together before either go into target area		Data Collector Log	RDD site
IA	12-May-03	16:34	FBI SIOC and DHS are considering redeployment of DEST		Data Collector Log	FBI SIOC
IL	12-May-03	16:35	ARC of Greater Chicago received notification from Chicago OEMC that alert status raised to Red		Data Collector Log	ARC of Greater Chicago HQ
IL	12-May-03	16:35	Director of Chicago OEMC advises that change to Red is unconfirmed; hold at Orange until HSAS notification		Data Collector Log	Chicago EOC
WA	12-May-03	16:35	FBI ASAC: DEST assets redeployed; Ce137 identified; TSA closed airports and airspace; upcoming press conference-not releasing anything of substance/no video		Analyst log	FBI Command Group Mtg
IA	12-May-03	16:35	INJECT: At the request of the Seattle SAC the SIOC requests DHS redirect the DEST to Seattle from the Columbia Generating Station in Hanford, WA.		TSA Daily Watch Log	DHS/CAT
WA	12-May-03	16:35	DOE Region 8 RAP Team receives call requesting assistance from WA DOH (corresponds to MSEL # 2037)	Time taken is from DOE RAP review comments. Other times recorded are from a WA SEOC data collector at 13:56 PDT (16:56 EDT); other times reported to the MSEL team are 13:00 and 13:57 PDT (16:00 and 16:57 EDT) from unknown sources.	AAR Review Comments	DOE RAP
IA	12-May-03	16:36	DOT CMC update: Washington State Ferry system shut down, FHWA reports I-5 is closed, I-90 is closed westbound / open eastbound near blast site.		Data Collector Log	DOT CMC
IA	12-May-03	16:37	DHS has activated NDMS		Data Collector Log	HHS
IA	12-May-03	16:37	DHS moving assets forward. On alert: 4 DMATs, NMRT-C, Region 10 DMORT, DPMU team, MST, DMORT WMD, IMSURT.		Data Collector Log	HHS
IA	12-May-03	16:37	HHS SCC noted that as yet there had been no Federal declaration--hence, OER advised against activation of ESF 8.		Data Collector Log	HHS
WA	12-May-03	16:39	SPD mobile command van now colocated with SFD mobile command van and SFD ICP		Data Collector Log	RDD site
IA	12-May-03	16:40	SIOC received report: Estimated 25 dead in Seattle blast area; blast zone is "hot"		Data Collector Log	FBI SIOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	16:42	Decision between SFD plans and SPD to combine both agencies planning processes together into a unified system		Data Collector Log	RDD site
IA	12-May-03	16:45	INJECT: DEST diverted to Seattle, WA. (MSEL # 3048)		ONCRC/USSS/DHS Activity Log	DHS/CAT
IA	12-May-03	16:45	INJECT: CDC & HHS ASPA craft an appropriate public health announcement in consultation with FBI JIC (MSEL # 3110)		Data Collector Log	HHS
IA	12-May-03	16:45	NNSA/HQ calls the NNSA/NV EOC to notify the CMRT Phase I and Phase II and the AMS (fixed-wing only) (corresponds to MSEL # 3132)		Data Collector Log	HHS
WA	12-May-03	16:45	At 13:45, the CST received notification from the WA SEOC to deploy to the incident site	The time used was from a post-exercise conversation with the CST Commanding Officer. The National Guard Component Log in the WA State EOC recorded this at 14:00 PDT (17:00 EDT)	Analyst Notes	CST Commanding Officer
WA	12-May-03	16:51	King County issued disaster declaration		Data Collector Log	FEMA Region X ROC
WA	12-May-03	16:54	FBI ASAC (Assistant Special Agent in Charge) and SPD IC have a discussion: There is no armed threat; SWAT and Bomb squads conducted secondary sweep. SFD cleared to go into hot zone for aid and rescue		Data Collector Log	RDD site
IA	12-May-03	16:58	Discussion in HHS SCC about declaring a Public Health Emergency	A Public Health Emergency was ultimately NOT declared for Washington	Data Collector Log	HHS
IL	12-May-03	17:00	Chicago EOC notifies Chicago DOT, Streets & Sanitation Dept., BOMA, Aon Center, Transunion building, IL Hotel & Lodging Assoc., North Michigan Avenue, Sears Building, Hancock Building, Merchandise Mart to suspend deliveries into buildings.		Data Collector Log	Chicago EOC
IA	12-May-03	17:00	INJECT: Consequence Management Agencies are notified to report to the SIOC (MSEL # 3401)		Data Collector Log	FBI SIOC
IL	12-May-03	17:02	IL SEOC confirms alert status still at Orange		Data Collector Log	ARC - Chicago HQ
WA	12-May-03	17:02	City employees are advised to stay at work and shelter in place until Seattle EOC receives further direction from the SFD		Agency Log	WA State EOC/Seattle EOC
IA	12-May-03	17:03	DOT CMC receives call from the Captain of the Port of Seattle: passenger ferry closed down as of 1515 EDT		Data Collector Log	USDOT HQ
IA	12-May-03	17:05	CDC Office of Communications begins coordination with HHS, Inter-agency JIC, and local/State public affairs offices to craft health communication messages.		Data Collector Log	CDC EOC Atlanta
IA	12-May-03	17:05	Hundreds of doses of Prussian Blue are en route to Seattle from DOE. They will arrive at 2100. Discussions at HHS SCC pointed out the facts that 1) this amount would only treat 250 people for one week, and that therefore ought to be limited to exposed responders, and 2) Prussian Blue only counters the radiation coming from the Cesium.		Data Collector Log	HHS
IA	12-May-03	17:05	DOE deliberating sending DTPA to Seattle. DTPA is only useful in the first 6 hours after exposure. So DTPA in Oakridge Stockpile won't get there in time.		Data Collector Log	HHS
WA	12-May-03	17:06	Press conference on VNN with Seattle Mayor: estimate 50-60 injured; tells citizens to "shelter in place" if they are located south of Royal Brougham - west of Rainier Street - north of S. Alaska - east of Duwamish Waterway including Harbor Island		Data Collector Log	Washington State EOC
WA	12-May-03	17:08	Seattle Mayor declares State of Emergency		Agency Log	WA State EOC/Seattle EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	12-May-03	17:10	EPA OSC report to EPA HQ: EPA responders to start perimeter monitoring; also suggests monitoring and tracking of 1st responders.		Data Collector Log	EPA EOC HQ D.C.
IA	12-May-03	17:10	NCEH is notified that FEMA Region X ROC had become operational as of 1100 EDT.		Data Collector Log	CDC EOC Atlanta
IL	12-May-03	17:11	Chicago EOC distributes information that HSAS level is still ORANGE		Data Collector Log	ARC - Chicago HQ
IA	12-May-03	17:17	FBI SIOC reports radioactive plume moving toward or near SeaTac Airport from downtown Seattle.		Data Collector Log	FBI SIOC
IA	12-May-03	17:19	FBI update: 4 male suspects - one suspect in custody by Seattle Police Department; 3 at large		Data Collector Log	FBI SIOC
IA	12-May-03	17:20	DHS Secretary receives letter from WA Governor requesting release of pre-positioned equipment package (PEP) in Seattle; letter is forwarded to CAT.		Agency Log	DHS/HS Center
IA	12-May-03	17:21	HHS sends blood donation coordinator to talk to VNN and rectify the story on need for blood		Data Collector Log	HHS
WA	12-May-03	17:25	AMS (Aerial Monitoring System) deployment order issued		Data Collector Log	WA State EOC
WA	12-May-03	17:32	Washington State Governor declares a State of Emergency in Western Washington in response to the explosion in Seattle (corresponds to MSEL # 2074). Text: I, Gary Locke, Governor of the state of Washington, as a result of the aforementioned situation and under Chapters 38.08, 38.52, and 43.06 RCW, do hereby proclaim that a State of Emergency exists in the Western Washington, and direct the supporting plans and procedures to the Washington State Comprehensive Emergency Management Plan be implemented. I also hereby order into active state service the Washington National Guard. I do hereby authorize the Washington Emergency Management Division to establish Food Control Areas around the areas that may be contaminated above protective action guidelines. The Washington State Departments of Health and Agriculture are authorized to issue food embargoes for the Food Control Area to reduce the possibility of adulterated food from leaving the Food Control Area. Law enforcement agencies are authorized to stop and inspect vehicles departing an identified Food Control Area and to direct the vehicle operators to return food produced or grown to its point of origin within the Food Control Area.	Time taken was from WA State EOC Log. Additional times include 14:22 PDT (17:22 EDT) from State EOC's EMACS Section log, 14:40 and 15:00 PDT (17:40 and 18:00 EDT) from MSEL Team logs.	Proclamation	WA State EOC
WA	12-May-03	17:34	DOH Representative at WA SEOC making request direct to FEMA for FRMAC team		Data Collector Log	WA State EOC
IA	12-May-03	17:35	DHS-CAT situation update report: FPS deployed to ROC, JOC, and all major federal locations in Seattle. FPS San Francisco is ready to send additional police officers to Seattle. Police officers were deploying with radiation detection devices to facilities northwest of the blast site and tracking prevailing winds.		Situation Report	DHS-CAT
IL	12-May-03	17:36	Kane County EOC reports that the Chicago EOC is up and running due to a possible attack in Chicago.		Data collector Log	Kane County EOC
IA	12-May-03	17:36	VNN report: Red Cross activates blood donor system.		Data Collector Log	HHS
IL	12-May-03	17:46	Kane Co. received EMNet Emergency Message that Lake Co. EOC has been partially activated because of Seattle bombing.		Data collector Log	Kane County EOC
WA	12-May-03	17:46	WA Governor's Proclamation of a State of Emergency forwarded to JOC		Washington National Guard Log	WA State EOC
IL	12-May-03	18:03	IEMA notified CCSEMA that the IL SEOC made a decision to shut down as of 17:00, lacking any definitive information or credible threat		Message & Event Log	CCSEMA

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	18:08	Seattle EOC requests DHS pre-positioned equipment package (PEP) located at Boeing Field		Data Collector Log	Seattle EOC
IA	12-May-03	18:10	Report to SIOC that Federal Hazmat teams, including first Federal radiation detection team, have arrived on-site in Seattle.		Data Collector Log	FBI SIOC
WA	12-May-03	18:11	Hospital control transferred to Overlake Hospital Medical Center from Harborview Medical Center due to broken water main at Harborview	Time chosen is when Overlake confirmed transfer of hospital control	Data Collector Log	Harborview EOC
IL	12-May-03	18:15	VNN reports that IL Governor has ordered increased security at nuclear power plants		SEOC Event Log	IL State EOC
WA	12-May-03	18:15	FRMAC authorized to deploy; estimated time of arrival in Seattle at 18:00.		FRMAC Log	FRMAC
WA	12-May-03	18:18	FBI Seattle ERT arriving at incident site		Data Collector Log	RDD site
WA	12-May-03	18:18	FBI California/San Francisco HMRT arriving on site		Data Collector Log	RDD site
IA	12-May-03	18:20	VNN report: Seattle hospitals receiving an overwhelming number of patients.		Data Collector Log	HHS
IL	12-May-03	18:29	Pro-Net alerts DuPage County Health Department to an increase in admissions of patients with respiratory complaints to Edward Hospitals		Detailed Incident Report	DuPage County EOC
WA	12-May-03	18:40	FBI HMRU arriving on site		Data Collector Log	RDD site
IA	12-May-03	18:45	SCC receives Seattle casualty update: 2 fatalities and 92 hospitalized.		Data Collector Log	HHS
IL	12-May-03	18:46	Chicago DPH decides to send out dirty bomb information to the public, but will wait to send out information on the alert status		Data Collector Log	Chicago DPH
IL	12-May-03	18:49	Blast fax sent to 34 hospitals on information about radiological dispersion devices and for hospitals to increase surveillance; took 49 minutes to transmit		Data Collector Log	Chicago EOC
WA	12-May-03	18:55	Hospital control transferred back to Harborview Medical Center		Incident Log	Harborview EOC
IA	12-May-03	19:02	HHS SCC set up the CDC Emergency Comms System, and modified its website to highlight radiation information.		Data Collector Log	HHS
WA	12-May-03	19:20	WA Governor signed the request for Presidential Disaster Declaration		Operations Section Activity Log	WA State EOC
IA	12-May-03	19:23	In the FBI SIOC, presentation of DHS's list of seven threatened cities (Seattle, Chicago, New York, Los Angeles, San Francisco, Houston, and the District of Columbia) resulted in a discussion of whether these cities were close to nuclear power sites. If so, FBI would recommend transition to Red.		Data Collector Log	FBI SIOC
IA	12-May-03	19:35	DHS Secretary declared HSAS RED in Seattle.		TSA Daily Watch Log	DHS/CAT
WA	12-May-03	19:36	HHS Secretary and DHS Secretary discuss the deployment of additional health physicists to WA		Data Collector Log	REOC
IL	12-May-03	19:40	Chicago OEMC sends message to RTA, CTA, METRA to bring trains down and start rush hour early. Contacted BOMA, Transunion building, Sears, Aon Center, Hancock Towers, Streets and Sanitation: no parking, etc.		Data Collector Log	Chicago EOC
WA	12-May-03	19:45	King County employees whose job site is located inside the effected zone are to shelter in place until otherwise advised. King County employees who live inside the zone cannot return to their homes. Employees are encouraged to follow the transit plan set out by King County Metro Transit.		Press Release	KC IC
WA	12-May-03	19:45	Global message to King County employees - King County employees are allowed to leave anytime but are encouraged to check the Employee Hotline, at 206-205-8600, the King County Web site, and watch the local news tomorrow morning for updates and information about reporting to work.		Press Release	KC IC
IL	12-May-03	19:47	Edward Hospital reports admission of family of four suspected of SARS, but with unusual coughing up of blood. DuPage County Health Dept. called IDPH and other five hospitals to alert them.		Detailed Incident Report	DuPage County EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	19:50	SPD requesting FBI assistance at scene of explosion.	Briefing occurred at 17:30 PDT (20:30 EDT). Action took place sometime between 16:50 and 17:30 PDT (19:50 and 20:30 EDT), when the briefing took place.	Intelligence Summary Report (ISR) Seattle Division	WA State EOC
IA	12-May-03	20:00	HHS SCC orders two SNS sites nearest Chicago to be readied for loading onto the airplanes.		Data Collector Log	HHS
WA	12-May-03	20:20	DHS Secretary, in consultation with Seattle Mayor, has declared HSAS Red for the Seattle/King County area	Also recorded by a data collector at the FEMA IOF	FEMA activity Log	WA State EOC
IL	12-May-03	20:21	Director of Chicago OEMC reports that a telephone call from Chicago Dept. of Health & Human Services has raised the alert status from Orange to Red. While awaiting confirmation by Fax; all Chicago OEMC personnel/agencies will implement Red Alert.	This actually reflects change in Chicago Health and Human Services alert status	Data Collector Log	Chicago EOC
IA	12-May-03	20:27	DHS-CAT reports that DHS has advised that effective at 2130 EDT, the alert level will be raised to RED for the following cities: Seattle, San Francisco, Los Angeles, Houston, Chicago, New York, Washington, D.C.		Situation Report	DHS-CAT
IL	12-May-03	20:32	Chicago area EOCs notified of elevation of HSAS to RED for seven high-risk cities.		Detailed Incident Report	DuPage County EOC
WA	12-May-03	20:40	FBI announced that incident is a terrorist event		Component Log	RDD Site
IA	12-May-03	20:46	HHS SCC gets word of the seven-city Red; will notify CDC to load the planes.		Data Collector Log	HHS
WA	12-May-03	20:50	SFD requested the release of DHS pre-positioned equipment package (PEP) located at Boeing field. Request passed to FEMA		Operations Log	WA State EOC
IL	12-May-03	20:56	Chicago Fire Dept informed by FBI Chicago that Chicago is listed as a "probable" target. Increase security for senior elected officials – Governor and Mayor. Specific threats have been identified.		Data Collector Log	Chicago EOC
IL	12-May-03	20:57	CPD recommend cancellation of White Sox baseball game and McCormick Place convention; Emergency Management Coordinator concurs. 12 hour shifts for sworn personnel; all in uniforms. Contact special details at O'Hare and Midway for Code Red protocols. Increased security for city target buildings.		Data Collector Log	Chicago EOC
WA	12-May-03	21:00	WA Hospital Control ceases operations		Incident Log	Harborview Hospital
IA	12-May-03	21:00	CDC operations center receives message from HHS SCC that 7 cities are now at threat level red. EOC staff notifies associated CDC staff members		Data Collector Log	CDC EOC Atlanta
IA	12-May-03	21:02	HHS, conferring with Chicago health officials, wants to pre-deploy the SERT now; it will be there by morning. In another matter, HHS will work with RHA to pre-position SNS stockpile near Chicago, based on information from British Columbia.		Data Collector Log	HHS
WA	12-May-03	21:10	SPD IC meet with Mayor and Chiefs at police command post; SPD IC advised that this was a terrorist event		Data Collector Log	RDD site
IA	12-May-03	21:10	FBI SIOC learns that 7 cities will go to Red at 2130.		Data Collector Log	FBI SIOC
IA	12-May-03	21:30	USSS Director's Crisis Center activated		Federal Response Briefing (Info Cut-Off Time: 0600 13 May 03)	DHS-CAT
IA	12-May-03	21:41	CDC putting out health alert to Chicago area doctors and hospitals. Plague is to be added to watch list, based on intelligence. But CDC is not suggesting an outbreak of this disease; the alert says to look for flu, or similar respiratory illness.		Data Collector Log	HHS
WA	12-May-03	21:44	Seattle Shelter-in-place press release approved		Press Release	Seattle EOC
IA	12-May-03	21:45	HHS SCC received notification from OER that NDMS teams were activated (notionally) in response to HSAS elevation to RED for the seven cities.		Data Collector Log	HHS
WA	12-May-03	22:00	US Coast Guard Seattle is at MARSEC 3 (highest level of security) - this means certain parts of the Port of Seattle are closed and port traffic is being directed to other locations		Situation Report 2	WA State EOC
WA	12-May-03	22:00	DEST arrives at the FBI Seattle Field Office (corresponds to MSEL # 3052).	Time taken from JOC analyst log. Other times reported 21:00 and 17:05 PDT (0:00 and 20:05 EDT) by MSEL Team from unknown sources.	Analyst Log	JOC CMG
IA	12-May-03	22:07	From EPA HQ: DOE designated as lead for radiological matters; other Federal agencies are to take DOE's direction on monitoring requests. DOE is to receive all data now, through the FRMAC, but data can be shared concurrently with State and local officials.		Data Collector Log	EPA EOC HQ D.C.
IA	12-May-03	22:30	FEMA EST and OSHA to coordinate an inter-agency health & safety plan		Data Collector Log	EPA EOC HQ D.C.
IA	12-May-03	22:30	First SNS situation report was issued by CDC. Primary area of coordination is supply of Prussian Blue, Ca DTPA or Zn DTPA.		Data Collector Log	CDC EOC Atlanta
WA	12-May-03	22:40	National Controller called WA SEOC Director to inject that the national threat level went Red, effective 1740 PDT.		Data Collector Log	WA State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	12-May-03	22:46	NRC alerts FBI information control that it is going to highest level security at nuclear power plants.		Data Collector Log	FBI SIOC
WA	12-May-03	22:58	FBI has completed trail vehicle evidence investigation. FBI identified GLODO involvement (corresponds to MSEL # 3051)	Time taken was from MSEL Team log (source RDD Site Controller). Additional time 21:30 PDT (0:30 EDT) from RDD Site Data Collector, identifying more actions than completion of vehicle evidence collection.	MSEL Team Log	MSEL
IL	12-May-03	23:00	IDPH put out fax alert regarding signs and symptoms (definitions of) of respiratory illness, fever, pain in the chest; 60 suspected cases		Fax Alert	IDPH
IL	12-May-03	23:00	DuPage County Public Health gets notification from IDPH of a TOPS cluster and passes this notification on to all offices and hospitals		Analyst Notes	IL VCC
WA	12-May-03	23:00	King County EOC talked to JOC: confirmed event designated as a terrorist incident and FBI assuming investigative lead.		Component Log	King County EOC
IL	12-May-03	23:00	Last night at 2200 - DuPage County notified from IDPH - notified of "TOPS" cluster - to all PH offices and hospitals		Data Collector Log	DuPage County PH
WA	12-May-03	23:10	Conference call with key state, county, and city players to update status of current situation: PHSKC EOC recommending: safe to remove shelter in place, but unsure how to transport those people out of Exclusion Zone. Will bring in buses from outside the Exclusion Zone to evacuate the public--tell them to go home, bag clothes, put in garbage, shower with water and soap, and await further instructions and info. Final Recommendation: risk of continuing to shelter in place is greater than contamination threat of leaving the area. But, want to transport people out of area using non-contaminated vehicles brought to perimeter of incident area		Data Collector Log	SKCPH EOC
IA	12-May-03	23:23	USMS reports Federal courthouse in Seattle is closed, but a magistrate remains on duty.		Data Collector Log	FBI SIOC
WA	12-May-03	23:30	Incident has been declared a criminal act; FBI has assumed control of the incident site		Data Collector Log	RDD Site
IA	12-May-03	23:30	Washington State request for Federal Disaster Declaration submitted to White House		Federal Response Briefing	DHS-CAT
WA	12-May-03	23:34	Incident Site Update: Command staff transition taking place; HazMat and technical rescue operations still on-going; new tents and lights being erected in command post area for night operations. SPD and SFD command posts side by side but separate. Still no unified command. Federal agencies on scene include FBI and EPA in command post area.		Data Collector Log	RDD site
WA	12-May-03	23:50	FBI has declared event a terrorist incident effective 20:00 PDT (23:00 EDT) & assumed lead investigative agency role. Investigation has associated a Maroon Honda & a blue GMC pick-up truck with the incident. Honda recovered near scene after crash with one non-identified suspect dead-on-arrival. Blue pick-up believed headed north-bound towards Canada.		King County OEM Event Log	KC EOC
WA	12-May-03	23:56	Data from AMS received by FRMAC.		Data Collector Log	FRMAC
WA	13-May-03	0:00	King County Situation Report - King County Metro Transit has made arrangements to provide Water Taxi service from West Seattle to downtown Seattle at 5:15 PDT (8:15 EDT) Tuesday.		Press Release	KC IC
IL	13-May-03	0:14	Central Dupage Hospital alerted Health Dept. of a suspected plague case	The evaluation team does not know if Health Dept. refers to the DuPage County Health Dept. or to IDPH (or both)	Detailed Incident Report	DuPage County EOC
WA	13-May-03	0:15	All patients have been rescued, rubble pile is clear of live victims		Data Collector Log	WA State EOC
WA	13-May-03	0:16	Ongoing discussions between WA SEOC, King County EOC, and Seattle EOC, and public health officials about shrinking the exclusion zone. There were repeated concerns about a lack of data.		Data Collector Log	KC EOC
WA	13-May-03	0:25	Conference Call between WA SEOC (including WA DOH), King County EOC, Seattle EOC, and PHSKC EOC to develop evacuation plan for people sheltering-in-place in industrial area of exclusion zone: First wash down evacuation route(s), coordinate buses into the incident area. SFD, SPD, and DOT available to support the evacuation. Evacuated people will be taken to a holding area, where relatives can come get them or they can go to shelters. At holding area, directions will be given to people about how to decontaminate at home (remove clothing, bag them, shower with soap and water). There is an unknown number of people in industrial area. Buses can transport 60 people at one time. All in area West of I-5 will be evacuated; will wait on more lab data before evacuating those East of I-5.		Data Collector Log	SKCPH EOC
WA	13-May-03	0:30	FBI has overall command and SFD has rescue command; FBI will be on scene all night		Data Collector Log	RDD site
WA	13-May-03	0:30	Unified meeting made up of SFD, SPD, and FBI, to discuss overall situation at incident site		Data Collector Log	WA State EOC
WA	13-May-03	1:00	FBI HMRU Leader's decision to have joint entry teams was based on number factors: Desire to facilitate interagency cooperation; evidentiary concerns with jurisdiction--the mixed teams would allow for a representative from agencies that claim to have jurisdiction of the evidence; levels of experience - some agencies have more experience with blast analysis.		Data Collector Log	RDD Site
WA	13-May-03	1:05	WA SEOC List of Priority Actions: 1) Radiation Footprint and impacts. 2) EST Recovery and Restoration Task Force. 3) Critical Infrastructure Protection. 4) Re-opening of I-5 5) Presidential Declaration		Data Collector Log	WA State EOC
WA	13-May-03	1:09	WA SEOC reports: SFD HazMat confirms detection of Americium 241 and Cesium 137 and relays to IC/ CPS		Data Collector Log	WA State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	13-May-03	1:30	Global e-mail to King County Employees: Only essential King County personnel who's job site is within the following boundaries--Royal Brougham to the North, I-5 to the East, S. Alaskan Way to the South, and Elliott Bay to the West--are being told to report to work tomorrow, Tuesday, May 13. Employees are advised to check with the King county employee hotline, at 205-8600, and the King County Website, at www.metrokc.gov for department specific information		Press Release	KC IC
WA	13-May-03	1:37	WA PFO priorities for night: defining the affected area, developing protective actions, and constructing a consistent message to the communities.		JOC CMG Log	JOC CMG
WA	13-May-03	1:48	SFD determined no viable victims left at incident site; switching from rescue mode to recovery mode.		FBI Log	WA State EOC
WA	13-May-03	2:00	Data from DOE AMS identified an alpha emitter. FRMAC therefore believes that the shelter in place zone is too small. Seattle's initial assessment was based on data from only a gamma emitter (Ce 137) at relatively low levels. FRMAC recommends to WA PFO that Seattle evacuates all people in exclusion zone, but need ground samples to determine exact measures. EPA's makes recommendation to wait until morning (since people are sleeping) when more data has come in--State and locals made the best decision they could with the information they had at the time. WA PFO's decision is to recommend to the city to maintain shelter in place until more data comes in; not to evacuate.		Analyst log	FRMAC briefing
WA	13-May-03	2:02	WA PFO learns that Seattle is planning to evacuate those civilians who have been sheltering in place in industrial area		Analyst log	FRMAC briefing
WA	13-May-03	2:10	WA SEOC faxes a request for the DMAT to the FEMA Region X ROC. They want a medical team to do enhanced primary medical care to augment overwhelmed local emergency departments due to potential affected population zone & "worried well" and screening for emergency reserve.		Fax	FEMA Region X ROC
WA	13-May-03	2:12	WA DOT: City of Seattle recommended opening of state highways, but they lack the authority to do so.	This occurred between 23:12-23:40 PDT (2:12-2:40 EDT)	Data Collector Log	WA State EOC
WA	13-May-03	2:50	Discussions ensue at the Seattle EOC about plans to decontaminate the streets by washing them down; concerns are raised about the sewage system, potential legal issues, and environmental impact	This occurred between 23:50-00:15 PDT (2:50:3:15 EDT)	Data Collector Log	Seattle EOC
WA	13-May-03	3:12	KC EOC reports that Seattle has put out a press release asking people to stay out of contaminated area, but people can go to work downtown.		Data Collector Log	KC EOC
IL	13-May-03	3:58	LaGrange Hospital evaluated current patients and identified a possible case of pneumonic plague		Data Collector Log	LaGrange Hospital
WA	13-May-03	4:00	Decision is made for the SFD to remain in charge of incident scene until 6:00 PDT (9:00 EDT) Tuesday when full FBI returns	This occurred between 01:00 and 01:30 PDT (04:00 - 04:30 EDT).	Data Collector Log	RDD site
WA	13-May-03	4:35	Plans to go forward with the evacuation of those sheltering-in-place in industrial area of exclusion zone is hampered by a lack of data.		Data Collector Log	WA State EOC
WA	13-May-03	5:00	WA SEOC recommends to USCG & Harbor Patrol to reopen the navigable waters for the following Washington State Ferries: vehicle and passenger service only on the Anacortes-San Juan, Edmonds-Kingston, and Fauntleroy-Vashon-Southworth; Passengers-only service on the Mukilteo-Clinton, Keystone-Port Townsend, and Port Defiance-Tahlequah routes. Recommend security measures in place for walk-on passengers to remain in effect.		Protective Action Decision Wksht	WA State EOC
WA	13-May-03	5:00	WA SEOC recommends that all existing highway closures remain in effect		Protective Action Decision Wksht	WA State EOC
WA	13-May-03	5:42	WA SEOC Press release: WA DOH to begin evacuation of immediate blast area. People will be notified by radio and by direct phone calls into the area west of I-5 using telephone numbers listed on business licenses in the city finance department. The area to be evacuated is bounded by Royal Brougham Way on the north, I-5 on the east, S. Alaska St. on the south, and the Seattle waterfront on the west.		Press Release	Seattle EOC
WA	13-May-03	6:28	WA SEOC notified that Seattle Mayor decided I-5 will re-open at 05:00 PDT (08:00 EDT)		Data Collector Log	WA State EOC
WA	13-May-03	6:28	Per WDOT, radiological data has not been confirmed. Therefore I-5 will remain closed.		EOC Supervisor Log	WA State EOC
WA	13-May-03	6:31	Seattle EOC: Retracted opening of I-5 until additional data from DOE AMS fly over comes in.		Agency Log	Seattle EOC
IA	13-May-03	7:10	HHS ASPHEP requests CDC to contact SERT leader in Chicago and tell him to request increased surveillance. CDC agrees to call Chicago.		Data Collector Log	FBI SIOC
WA	13-May-03	7:15	SFD IC & Operations Chief meet face to face with NMRT. NMRT tasked with force protection		Data Collector Log	WA State EOC
WA	13-May-03	7:37	WA SEOC requests Fire Mobilization Authorization on behalf of SFD		Public Information Officer's Log	WA State EOC
WA	13-May-03	7:45	WA SEOC News Release: WA State Ferries to resume full service except for Seattle runs.		Public Information Officer's Log	WA State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	13-May-03	8:05	NCEH, lead CDC center responding to radiological event, conducts conference call with Seattle & King County EOCs, Regional X REOC, and CDC's A-team representatives.		Data Collector Log	HHS - SCC
IL	13-May-03	8:10	ARC of Greater Chicago received a phone call from IL SEOC: confirmed Red Alert for IL became effective at 19:00 CDT (20:00 EDT) on Monday. Also informed that IDPH has reported about 100 patients with SARS-like symptoms have reported to Chicago hospitals. Due to this, ARC will discontinue blood collections in this area. All chapters will be notified of alert status. National ARC "Get Info Public" info line has been activated		Data Collector Log	ARC of Greater Chicago HQ
WA	13-May-03	8:30	WA SEOC News Release: WA Governor appointed a Recovery and Restoration Task Force to guide and coordinate state government recovery efforts in areas of King County and Seattle affected by the explosion		Press Release	WA State EOC
IA	13-May-03	8:38	FEMA HQ calls for a CDRG meeting at 0900 on May 13, 2003		Data Collector Log	EPA EOC HQ D.C.
IL	13-May-03	8:45	DuPage County Public Health Dept. goes on 24/7 ops		Data Collector Log	DuPage County PH
IL	13-May-03	8:45	Highland hospital received clarification from IDPH that it wasn't the alert level that went to red; it was the infection alert level		Analyst Notes	IL VCC
IL	13-May-03	8:58	DuPage County Public Health to get surveillance teams up and going		Data Collector Log	DuPage County Health
WA	13-May-03	9:00	WA SEOC was notified by FEMA Region X Liaison that the PDD was signed at 900 EST on May 13. WA SEOC is trying to obtain a copy of signed declaration at this time. Disaster number will be DR-4321-WA.		Situation Report	WA State EOC
IA	13-May-03	9:12	HHS SCC holds a conference call with Region V to discuss biological event. Key discussion points: NCID is the lead CDC center supporting the bio event; needs to engage State & local health officials to convey prophylaxis strategies. Communications staff coordinate with locals to develop messages for media and public.		EP&R activity log	DHS/ HS Center
IL	13-May-03	9:15	CCDPH begins active surveillance. Contact Chicago hospitals by fax, but don't discuss disease with public yet.		Data Collector Log	CCDPH
WA	13-May-03	9:15	FBI locates two safehouses (corresponds to MSEL # 3053)	Time taken was from a RDD site controller log. Other times listed by MSEL Team were 21:40 and 22:30 PDT on May 12 (0:40 and 1:30 EDT on May 13) from unknown sources.	Controller Log	RDD Site
WA	13-May-03	9:15	Seattle Mayor signed a general exclusion order, which restricted public access in an area bounded by S Horton St. on the South, SR99 on the West, Royal Brougham on the North, and Airport Way on the East.		Seattle EOC Situation Report	Seattle EOC
IL	13-May-03	9:23	DuPage County DPH alerts pre-selected prophylaxis dispensing sites to be prepared to be activated in the event that the IL Stockpile or SNS is requested.		Data Collector Log	DuPage County PH
IL	13-May-03	9:30	Chicago Dept. of Public Health dispatches epidemiology teams to 34 Chicago city hospitals		Data Collector Log	Chicago EOC
IL	13-May-03	9:30	Lake Forest hospital received fax confirming pneumonic plague. Fax also received regarding patient flow.		Data Collector Log	Lake Forest Hospital
IA	13-May-03	9:30	DOS stood up task force to liaison with Canada. Border security heightened ; Canadians are intercepting Seattle flights for possible decontamination.		Data Collector Log	CDC EOC Atlanta
IL	13-May-03	9:37	Chicago EOC has received only three reports from 3 hospitals; Chicago DPH to send staff out to hospitals to do face-to-face to emphasize increased reporting. Chicago DPH advising M-95 masks and infection control procedures for emergency responders.		Data Collector Log	Chicago EOC
IL	13-May-03	9:39	Chicago EOC pre-positioned specialized teams (hazmat, dive, rescue); locked down firehouses; activated secondary command post at Fire Academy.		Data Collector Log	Chicago EOC
IL	13-May-03	9:39	IDPH activates Phase I of IL Emergency Medical Disaster Plan. POD hospitals activated.		Data Collector Log	DuPage County Health

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	13-May-03	9:40	Loyola University Medical Center activated as a POD Hospital		Data Collector Log	Loyola Univ. Medical Center
IL	13-May-03	9:43	Chicago EOC notified Mayor's Chief of Staff and brought Mayor up to date; in contact with the IL Governor's Office; more senior staff reporting to EOC; preparing Chicago Declaration of Emergency draft.		Data Collector Log	Chicago EOC
IL	13-May-03	9:45	Highland Park hospital received call from IOHNO to go to Phase I of IL Emergency Medical Disaster Plan - must report back to IOHNO 10:30 CDT (11:30 EDT) that plan is implemented.		Data Collector Log	Highland Park Hospital
IL	13-May-03	9:45	Masonic ER reported to IDPH that Phase I of IL Emergency Medical Disaster Plan activated.		Data collector Log	Masonic ER
IL	13-May-03	9:50	IDPH has reported two cases of pneumonic plague in the Chicago area		SEOC Event Log	IL State EOC
IL	13-May-03	9:51	IL SEOC Director spoke with ISP Director and reported to IL SEOC: Based on intelligence information last night the North and Central (with the Southern team in reserve) SWMDT, National Guard 5th Civil Support Team, and IMERT are being activated. ISP will contact their members and IEMA to make remainder of contacts. They are to report to the College of DuPage. IL SEOC Director also authorized the activation of these special teams.		SEOC Event Log	IL State EOC
IL	13-May-03	9:55	IL SEOC notifies ARC Chicago District Operations Center of 2 cases of pneumonic plague, in addition to SARS - like patients presenting at hospitals over-night. Also notifies that IL SWMDT has been set-up in Dupage County		Data Collector Log	ARC - Chicago HQ
IL	13-May-03	9:55	Good Samaritan called Elmerst Memorial Hospital ER to tell charge nurse that Phase I of IL Emergency Medical Disaster Plan was implemented.		Data Collector Log	Elmhurst Memorial Hospital
IL	13-May-03	10:00	IDPH conference call with IDPH Lab: Top Priority for hospital labs is if they see bipolar staining using Gram stain and patients fit clinical picture; sputum samples, Bronchoalveolar Lavage, lung aspiration, Antibiotic susceptibility.		CCDPH Log	Cook County DPH
WA	13-May-03	10:00	Threat update: State of Washington, orange. City of Seattle, red; King County, red-based on local policy		EOC Supervisor Log	WA State EOC
IA	13-May-03	10:00	HHS Homeland Security Center Incident Report: All NDMS assets have been put on alert per the EP&R Response Division; Additional information from Chicago indicates at least 100 patients with SARS-like illness in Chicago; Epidemiologist in the Chicago area and has deployed to the Illinois Department of Health.		Data Collector Log	MCC
IA	13-May-03	10:00	NRC has increased security at power plants in their 4 regions as a result of DHS going code red. They will give any appropriate information to SIOC information control if necessary.		Data Collector Log	VA Central Office
IA	13-May-03	10:00	Canadians requested that they be allowed to send a liaison to Region X ROC; US Government has no objections.		Situation Report	DHS CAT
IL	13-May-03	10:02	Lake County DPH reports: Hospitals have said that patients who went to United Center are being reported as suspect SARS. Some cases were also at O'Hare Airport. DuPage Hospital suspects plague at 23:42 CDT on May 12 (0:42 EDT on 13 May). Some patients from Canada. DuPage: 13 suspect cases respiratory illness United Center Connection, O'Hare Connection, and Canada Connection		Data Collector Log	Lake County Dept. of Health
IL	13-May-03	10:04	Illinois Masonic activates Phase I of IL Emergency Medical Disaster Plan. Illinois Masonic faxed Swedish Covenant Phase I information sheet because they did not have it, though they are supposed to.		Data Collector Log	Swedish Covenant
IL	13-May-03	10:05	IDPH faxed LaGrange ER to implement Phase I of IL Emergency Medical Disaster Plan - charge nurse calling units and departments to determine beds, blood, vents - etc.		Data Collector Log	LaGrange Hospital
IL	13-May-03	10:15	Central DuPage Hospital activates Phase I of IL Emergency Medical Disaster Plan		Data Collector Log	Central DuPage
IL	13-May-03	10:20	VNN reporting unusual number of flu-like illnesses in Vancouver		Data Collector Log	IDPH
IA	13-May-03	10:20	NRC member of CAT requests copy of ARAC plots		Data Collector Log	FBI SIOC
IL	13-May-03	10:25	Northwest Community Hospital reported to Good Shepherd Hospital via radio that Phase I of IL Emergency Medical Disaster Plan implemented.		Data collector Log	Good Shepherd
IL	13-May-03	10:25	IL Governor has approved the deployment of the National Guard CST		SEOC Event Log	IL State EOC
WA	13-May-03	10:27	WA SEOC: PIOs instructed to NOT disseminate plume data to the media as it is not confirmed		Data Collector Log	WA State EOC
IL	13-May-03	10:30	American Red Cross of Greater Chicago PIO receives request from FEMA to go to the IL JIC		Data Collector Log	ARC - Chicago HQ

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	13-May-03	10:30	IDPH (Springfield): all lab specimens need to be expedited to IDPH Lab for definitive diagnostic testing		Data Collector Log	IDPH
IA	13-May-03	10:30	Homeland Security Center update: CDC recommends starting with Ciprofloxacin and then switching to Doxycycline later if advisable to do so; Several people have arrived in BC with have flu-like illness, on a flight originating from Chicago; HHS working to get SNS moved on a minute's notice.		DOE activity log	DHS/HS Center
IL	13-May-03	10:32	DuPage County DPH suggests dispatch IL State Police or local police as couriers to expedite lab analysis		Data Collector Log	DuPage County PH
IL	13-May-03	10:36	Lake County Health EOC advises Lake County EOC: 89 cases in Chicago area - 1 death from respiratory illness. Samples sent to IDPH Lab - preliminary results by noon - possible outbreak of plague per CCDPH. 10 may have been at United Center.		Data Collector Log	Lake County EOC
WA	13-May-03	10:40	Debriefing meeting with IC: Transitioned from rescue to recovery at 06:00 PDT (09:00 EDT). FBI taking over responsibilities for incident management. Scene monitoring (contaminants) still being performed by SFD HazMat. Decontamination responsibility transferred to NMRT. Jurisdiction over deceased discussed. DMORT on site by 11:00.		Data collector log	RDD Site
IL	13-May-03	10:41	IDPH: Prioritize specimens by bipolar staining or connection with United Center		Data Collector Log	IDPH
IL	13-May-03	10:47	Finalized "TOPS" case definition describing signs and symptoms of infectious disease trend beginning to appear.		Data Collector Log	IDPH
IL	13-May-03	10:54	IDPH notified ARC Chicago they have activated Phase 1 of their Emergency Medical Disaster Plan - IDPH collecting data and checking hospital space		Data Collector Log	ARC - Chicago HQ
IL	13-May-03	10:56	ARC of Greater Chicago reports that the early clinical diagnosis from the IL SEOC is incorrect; there is not enough information to confirm Plague		Data Collector Log	ARC - Chicago HQ
IA	13-May-03	10:57	Seattle FDA office preparing an advisory for consumers; blanket embargo of all foodstuffs in the plume area.		Data Collector Log	VA Central Office
WA	13-May-03	10:59	AMS fly over readings: Kitsap County (WA) readings are above food control limit; I-5 is clean, but people could drive into unsafe areas - so not ready to open. City requests making residential area east of I-5 a priority for measurement.		Data Collector Log	WA State EOC
IA	13-May-03	11:00	HHS/ SCC holds conference call with CDC and other ESF-8 partners; key discussion points: NCEH (CDC radiation lead) has posted worker safety radiation literature on CDC's website (some information is actually on the site, while other information is notionally posted). HHS SERTs sent to Seattle and Chicago. Reviewed current mission assignments/requests for assistance for the states. Seattle has requested the following ESF-8 assets: DMAT, NMRT, DMORT and the WMD DMORT. Additionally, CDC provided A-Team members to support FRMAC.		Data Collector Log	HHS - SCC
IL	13-May-03	11:05	CCDPH: indications that additional cases were presenting with symptoms and specimens consistent with plague, but no clear indication that's what it is. Cases showing from O'Hare and Union Station in addition to United Center.		Data Collector Log	CCDPH
IL	13-May-03	11:09	Chicago EOC update: FBI is at the EOC; 2 hospitals (Gottlieb and Ingalls) report clinical plague cases at hospital - the cases come from far south and far west of Chicago, but both attended recent event at the United Center; the HAZMAT Chief and City of Chicago notified.		Data Collector Log	Chicago EOC
IL	13-May-03	11:10	CCSEMA receives IEMA SitRep: at 09:15 CDT (10:15 EDT) IL State WMD team & IMERT were activated and ordered to assemble at College of DuPage		Message & Event Log	CCSEMA
IA	13-May-03	11:13	2nd SERT team is arriving soon in Illinois; will get additional epidemiological support from CDC.		Data Collector Log	DHS CAT
IA	13-May-03	11:20	Director CDC public health priorities: Focus on immediate needs of Chicago and Seattle - but do not over-commit CDC resources, as we need to consider the potential for multiple events in other parts of the country. Ensure the public health community stakeholders have the requisite information to stay informed as to what is happening. NCID staff needs to strategize on the potential diagnosis of plague, and be ahead if in fact the agent proves to be plague.		Data Collector Log	VA Central Office
IL	13-May-03	11:30	VNN announces patients with flu-like symptoms - possible SARS cases - in Chicago; unconfirmed deaths		Data Collector Log	ARC of Greater Chicago HQ
IL	13-May-03	11:32	At IDPH Lab, suggestion made to utilize "police" to get specimens from hospitals to IDPH lab.		Data Collector Log	IDPH lab
IL	13-May-03	11:40	Briefing at Chicago 911: confirmed pneumonic plague at Gottlieb Hospital in Melrose Park, Ingalls - Harvey and Childrens Hospital-Chicago. FBI notified Chicago Fire Department that the commonality is the Chicago United Center. Chicago Fire Department is sending teams to identify if bacteria still present.		SEOC Event Log	IL State EOC
WA	13-May-03	11:40	Red Cross representative to WA JOC CMG: King County Parks Dept. with support from ARC opened 3 shelters at 20:00 PDT on May 12 (23:00 EDT) for individuals unable to return to their homes.		JOC CMG Log	JOC CMG
IA	13-May-03	11:40	INJECT: FBI Chicago Field Office notified that CDC deploying assets to area (MSEL 3129)		Data Collector Log	CDC EOC Atlanta
IA	13-May-03	11:56	TSA liaison to FBI SIOC: New TFR will be announced with 5 mile radius, 18,000 feet (reduced from 20,000 ft)		Data Collector Log	FBI SIOC
IL	13-May-03	12:00	VNN confirms GLODO has claimed responsibility for Seattle attack		Data Collector Log	ARC - Chicago HQ
IL	13-May-03	12:00	Chicago DPH looking to identify travel history of all patients.		Data Collector Log	Chicago DPH

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	13-May-03	12:00	ESF 10 reports missing shipment of nuclear material	Also reported to FBI SIOC	Data Collector Log	FEMA EST
IL	13-May-03	12:04	CCDPH Conference call with Chicago and Collar Counties: Reports coming from hospitals, but do not have active surveillance. EIS officers will be going out in the field following conference call. State recommends that interviews should ask whether they have had exposure to O'Hare, Union Station, or United Center		CCDPH Player Log	Cook County DPH
IL	13-May-03	12:04	CCSEMA receives Sitrep from CCDPH: at 10:20 CDT (11:20 EDT), IDPH has made a presumptive diagnosis of 2 cases of pneumonic plague. DHS notified & SNS placed on standby.		Message & Event Log	CCSEMA
IL	13-May-03	12:05	VNN: IL Governor press release announcing confirmation of pneumonic plague cases and that state disaster plan has been implemented		Data Collector Log	Springfield IDPH
IL	13-May-03	12:07	IL Governor announces respiratory illness clusters in Chicago area. No evidence that illness is related to Seattle attack, but IDPH and other public health departments are working to determine cause of illness - urges citizens to take precautions.		Data Collector Log	ARC - Chicago HQ
WA	13-May-03	12:09	"There are no confirmed dead" - per King County Medical Examiners office, who received information directly from the IC		Data collector log	SKCPH EOC
IL	13-May-03	12:12	Chicago EOC: Plague is strongly suspected. Looks like plague under microscope; several cases known; many cases coming in right now. IDPH has 109 cases, Chicago had 5 cases, other counties have more. Chicago OEMC wants real numbers as soon as possible.		Data Collector Log	Chicago EOC
IL	13-May-03	12:13	Director Chicago OEMC: Via FBI Chicago, respiratory patients from O'Hare and Union Station at Lincoln Hospital. Chicago Fire Dept. to do investigative bio survey at O'Hare and Union Station. Plague presumed until further notice.		Data Collector Log	Chicago EOC
IL	13-May-03	12:14	IL SEOC received EMNet message. Information that IDPH has made a presumptive diagnosis of 2 pneumonic plague cases. The Department of Homeland Security has been notified; the national pharmaceutical stockpile (SNS) to be on standby.		SEOC Event Log	IL State EOC
IL	13-May-03	12:15	Chicago EOC received EMNet Emergency Message: IDPH has made presumptive diagnosis of 2 pneumonic plague cases. Chicago Dept. of Health & Human Services has notified SNS to be on standby for release.		Data Collector Log	Chicago EOC
IL	13-May-03	12:17	Lake County EOC: IDPH has made presumptive diagnosis of pneumonic plague.		Data Collector Log	Lake County EOC
IL	13-May-03	12:18	Lake County EOC notified emergency stockpile (SNS) to stand by		Data Collector Log	Lake County EOC
IL	13-May-03	12:20	IL JIC confirms reports of plague.		Data collector Log	DuPage Co. EOC
IL	13-May-03	12:36	CCDPH directed staff to develop public information message and get a phone bank ready and notify the Bridgeview distribution site, red cross, sheriff, public health clinics, and the PIO at the IL JIC		Data Collector Log	CCDHP
IL	13-May-03	12:40	Chicago 911 Briefing: City of Chicago putting together Disaster Declaration based on their activities dealing with health symptoms. 53 yr. female and 57 year male United Flight attendant both confirmed dead by Cook County medical examiners. Chicago in communication with Vancouver because Vancouver played Chicago Black Hawks this past weekend. Chicago Fire Department, Chicago Bomb Squad, and FBI are checking United Center, Union Station, and O'Hare Airport. Considering a request for CST team.		SEOC Event Log	IL State EOC
IL	13-May-03	12:45	Chicago EOC update: State of Emergency to be declared in in Chicago, recommend public Shelter-In-Place, Strategic National Stockpile requested. Final trigger was a message from Vancouver saying that their initial cases all came from Chicago and that their microbiologists/labs had confirmed Pneumonic Plague.		Data Collector Log	Chicago EOC
IL	13-May-03	12:46	Kane County EOC received an e-mail from IOHNO - WMD Civil Support teams and IMERT activated and are to stage at college of DuPage		Data collector Log	Kane County EOC
IL	13-May-03	12:58	Cook County EOC preparing proclamation of disaster		Data Collector Log	Cook County EOC
IA	13-May-03	12:59	HHS reported 2 cases with presumptive plague diagnosis and 100 additional sick with flu-like symptoms in Chicago. CDC is at the scene with an investigative team. DHS is conducting conference calls to confer on preparation activities.		Situation report from Bureau of Immigration and Customs Enforcement Headquarters Reporting Center	DHS/CAT
WA	13-May-03	13:00	HHS Region X REOC (WA) developing registry for people who were exposed. The Agency for toxic substances and disease registry (ATSDR) estimated 120,000 exposed people, Region X REOC (WA) believes this is probably too high		Data Collector Log	REOC
WA	13-May-03	13:00	Incident site update from WA SEOC: 21 dead on site, injured 51 Red, 43 Yellow, and 45 Green; Working with Seattle EOC to validate numbers.		EOC Supervisor Log	WA State EOC
WA	13-May-03	13:05	FBI determined that bomb went off accidentally; may be some other targets or explosives enroute		Analyst log	FSL Conference Call
IL	13-May-03	13:07	Director Chicago OEMC made big announcement - Declaration of State of Emergency in Chicago recommended; Chicago will order shelter-in-place; Chicago Law Department says: declaration of emergency gives authority to take necessary actions immediately. Press Conference will make announcement.		Data Collector Log	Chicago EOC
IL	13-May-03	13:09	IDPH approved memo describing treatment guidelines		Data Collector Log	Springfield IDPH

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	13-May-03	13:20	From DHS liaison to SIOC: NRC reports employees of a nuclear facility near Chicago are calling in sick. All of the employees had attended the Chicago Blackhawks game on May 10th. The Blackhawks played Vancouver. In addition 10 percent of the NRC Region III staff called in sick.		Data Collector Log	FBI SIOC
IL	13-May-03	13:20	CFD Chief says, "Field tested at O'Hare, Union Station, and the United Center." Not located any devices; will send swab sample to IDPH lab for culture. Swabbed HVAC system and common areas. Samples to be sent to IDPH laboratories; 48-hour turnaround. CSTs asked to be available to come in and support; on stand-by basis right now. CST has relocated from Peoria to College of DuPage.		Data Collector Log	Chicago EOC
IL	13-May-03	13:20	Chicago EOC talked with IDPH laboratory; They feel that outbreak started on Mother's Day; hazmat unit ran field tests; these field tests compromised by good housekeeping. Also, 48-hour turnaround for samples can be reduced to 3 hours.		Data Collector Log	Chicago EOC
IL	13-May-03	13:20	IDPH lab told that HazMat would organize site checks but based on clues thus far sounds like aerosol exposure. IDPH lab advising HazMat to look for possible devices and to collect perhaps little samples. HazMat believes based on clues/don't expect to find anything - will sample both ends of ventilation system for residual material. Will not do field analysis/will send samples direct to lab. Interagency teams will scour 3 sites for devices.		Data Collector Log	IDPH lab
WA	13-May-03	13:20	Federal JIC (WA) determines that VNN put out erroneous information; VNN announced that DHS was providing Prussian Blue at request of state, but state did not request from Oak Ridge; Oak Ridge automatically brings it.		Data Collector Log	JIC (WA)
IL	13-May-03	13:21	Cook County Epidemiology field teams are out and sending case reports to the state		Data Collector Log	CCDHP
IA	13-May-03	13:21	HHS ASPHEP wants paperwork for declaration of Public Health Emergency ready for the HHS Secretary to sign during briefing with President.		Data Collector Log	HHS - SCC
IL	13-May-03	13:27	IDPH lab reporting <i>Yersinia pestis</i> positive samples to IOHNO then to IDPH Springfield.		Data Collector Log	IDPH lab
IL	13-May-03	13:28	IDPH receives confirmation from lab - PCR tests completed; positive for <i>Y. pestis</i> (3 patients)		Data Collector Log	IDPH
IL	13-May-03	13:30	IOHNO receives confirmation from Chicago IDPH Lab - positive for plague (<i>Yersinia pestis</i>) based on PCR test of 3 specimens from Edwards Hospital. No press release yet!		Data Collector Log	IOHNO
IL	13-May-03	13:30	IL Governor declares state of emergency, requests activation of the SNS, mobilizes IEMA & IDPH.		Data Collector Log	Lake County EOC
IA	13-May-03	13:30	HHS ASPHEP: Based on the evolving numbers and a conference call with the DHS Secretary, the illness should be assumed to be plague and intentionally released.		Data Collector Log	FEMA HQ EST
IL	13-May-03	13:34	Chicago EOC received faxes from EMNet Emergency Message regarding activation of Strategic National Stockpile.		Data Collector Log	Chicago EOC
IL	13-May-03	13:35	IDPH activates Phase II of IL Emergency Medical Disaster Plan in response to Governor's Emergency Declaration.		Data Collector Log	Highland Park Hospital
IL	13-May-03	13:36	Plague confirmed - gram (-) rods		Data Collector Log	Sherman
IL	13-May-03	13:40	Elmhurst Hospital received fax from Good Samaritan Hospital instructing them to complete the Phase II worksheet.		Data Collector Log	Elmhurst Memorial Hospital
IL	13-May-03	13:40	IDPH notified Ingalls Hospital of code 99 (Phase II of IL Emergency Medical Disaster Plan)		Data Collector Log	Ingalls Hospital
IL	13-May-03	13:40	Northwestern Memorial Hospital and the University of Chicago-associated hospitals activated Phase II of IL Emergency Medical Disaster Plan		Data collector Log	Masonic ER
IA	13-May-03	13:40	HHS ASPHEP asks CDC to look at ventilators as part of their mobilization strategy.		Data Collector Log	HHS - SCC
IA	13-May-03	13:40	HHS SCC tasking ASPA to draft talking points regarding shelter-in-place, clarifying that they are NOT recommending sheltering-in-place nationwide.		Data Collector Log	HHS - SCC
IA	13-May-03	13:40	British Columbia & CDC confirms pneumonic plague; unconfirmed reports say that all of the sick people were on Air Canada flight 783 from Chicago. Legal will confirm and report back to FBI Chicago		Data Collector Log	HHS - SCC
IA	13-May-03	13:41	VNN report: DHS Secretary, on phone interview, was asked what should people in Code Red cities should do - urged people to minimize public activity and keep children at home. HHS ASPHEP recommends that people "take a snow day."		Situation Report	DHS-CAT
IL	13-May-03	13:45	Loyola University Medical Center activated Phase II of IL Emergency Medical Disaster Plan		Data Collector Log	Loyola Univ. Medical Center
IL	13-May-03	13:45	Sherman Hospital activated Phase II of IL Emergency Medical Disaster Plan		Data Collector Log	Sherman
IL	13-May-03	13:46	Declaration of disaster signed by Lake County Board Chairman		Data Collector Log	Lake County EOC
IA	13-May-03	13:49	Coast Guard closed all vessel traffic in the Port of Chicago.		Situation report from BICE HQ Reporting Center	DHS-CAT

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	13-May-03	13:50	Lake County EOC PIO tells the Lake County PIO at the IL JIC not to issue a press release of declarations of emergency until all counties release a declaration		Data Collector Log	Lake County EOC
IL	13-May-03	13:51	University of Chicago called to notify South Shore Hospital of activation of Phase II of IL Emergency Medical Disaster Plan . Phase II worksheet filled out by ED supervisor.		Data Collector Log	South Shore
IL	13-May-03	13:55	VNN report: IDPH says probably plague & Canadian officials confirm plague		Data Collector Log	ARC of Greater Chicago HQ
IA	13-May-03	13:55	CDC issues Health Advisory #3, suspect pneumonic plague cases reported in IL.		Data Collector Log	FBI SIOC
IA	13-May-03	13:55	HRT/BDC deployment approved by FBI HQ in accordance with HRT deployment directives.		Region X ROC input to EP&R situation report	DHS/HS Center
IL	13-May-03	13:58	VNN report: DHS Secretary terms preliminary diagnosis of Flu-like symptoms as "plague"		Data collector Log	Kane County EOC
IL	13-May-03	13:59	ARC of Greater Chicago observes DHS Secretary on VNN announce that IDPH has a preliminary finding of plague-like illness - urges residents to restrict movement and stay inside. Vancouver has confirmed plague so Chicago must work on assumption of plague. ARC administration discusses the mismatch between the information in the Secretary's speech and other sources confirming plague.		Data Collector Log	ARC - Chicago HQ
IL	13-May-03	14:00	200 National Guard personnel requested to assist the Medical Examiner in morgue duties; report to Police Areas Centers 1 through 5, First Police District, O'Hare Airport, Midway Airport.		National Guard Request, Police Department	Chicago DPH
IL	13-May-03	14:00	VNN report: DHS Secretary announces plague in Vancouver and also probably in Chicago; recommends public treat it as a "snowday".		Data Collector Log	IDPH
IL	13-May-03	14:10	IDPH Springfield: Recommend IL Governor request National Disaster Medical System (NDMS) and DMAT (need epidemiologic specialists to assist with disease investigations).		SEOC Event Log	IL State EOC
IL	13-May-03	14:12	VNN report: 14 confirmed dead in Chicago.		Data Collector Log	IOHNO
IL	13-May-03	14:17	IDPH arranging web posting of memos on treatment and prophylaxis		Data Collector Log	IDPH
IA	13-May-03	14:22	HHS confirms 14 dead in Chicago from SARS-like illness		EP&R activity log	DHS/HS Center
IL	13-May-03	14:30	FBI Chicago confirming Pneumonic Plague		Data Collector Log	Chicago EOC
WA	13-May-03	14:31	DHS is working on a FRMAC transition plan for lead to shift to EPA from DOE		Data collector log	EPA - RCC
IL	13-May-03	14:38	DuPage County DPH: Plague identified; next steps are to get information out and do contact tracing		Data Collector Log	DuPage County Health
WA	13-May-03	14:40	WA SEOC looking to verify casualty numbers from incident site; number Seattle is putting out is different than what King County is putting out		Data Collector Log	WA State EOC
IA	13-May-03	14:50	CDC EOC: Seattle update - Two confirmed fatalities; 1,200 people evacuated, 600 decontaminated, 41 in critical condition in area hospitals.		Data Collector Log	CDC EOC Atlanta
WA	13-May-03	15:02	Unified Command Brief: Hazmat teams following ERT in rubble. Cadaver dogs on site. Evidence collection to begin soon. FEMA, EPA, and DOE still in support. After bodies have been cleared, will shift focus to long range remediation		Data Collector Log	RDD site
IA	13-May-03	15:08	Federal Radiological Monitoring and Assessment Center (FRMAC) has advised that they completed aerial measurements and ground samples of radiation. The radiation does not pose an immediate threat to life or safety; people within the shelter-in-place area could stay in place for up to a year without exceeding EPA protective action guidelines for radiation dosages; FPS has already evacuated the Federal facilities that had sheltered in place. GSA & FPS did develop a list of people that were sheltered in the Federal buildings as a precaution for future medical review.		Situation report from BICE HQ Reporting Center	DHS/CAT
IA	13-May-03	15:09	CDC (NCID) receives notification from Chicago of PCR confirmation of plague		Data Collector Log	MCC
IL	13-May-03	15:11	DuPage County begins distribution of their pharmaceutical stockpile based on Governor's request for SNS.		Data Collector Log	DuPage Co.
WA	13-May-03	15:15	News release from KC Regional JIC: The State Department of Agriculture has announced that precautionary measures are recommended for the areas: East of the King County /Kitsap County border between N.W. 85th Street and S.W. Admiral Way; South and west of 85th Street to 24th Avenue N.W. to 65th Avenue N.W. to 15th Avenue N.W. to Highway 99 to Denny Way to Interstate 5 to Interstate 90 to Highway 900; North and west of South Columbia Way from Highway 900 to 15th Avenue to South Nevada Street to 4th Avenue to Dawson Street to Highway 99 to Spokane street to S.W. Admiral way to the King/Kitsap County Border. Specific precautionary measures include the following: Avoid purchasing or consuming products stored in open-air markets after 12:10 pm on May 12, 2003; Fruits, vegetables or grain should not be picked; Shell fish harvested after 12:10 p.m. on May 12, 2003 should not be harvested or eaten; Agricultural products should not be transported uncovered through the advisory area; Pets should be restricted to water sources that are covered or are from enclosed underground storage.		Press Release	KC Regional JIC
IA	13-May-03	15:15	CDC EOC confirming 3 cases of plague in Chicago, confirmed by PCR from CRN lab in Chicago.		Data Collector Log	CDC EOC Atlanta

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	13-May-03	15:20	Elmhurst Memorial Hospital receives fax from IDPH regarding signs and symptoms of infectious disease trend beginning to appear. Emergency management coordinator and charge nurse notified by ER staff who also notified infectious control nurse.		Data Collector Log	Elmhurst Memorial Hospital
WA	13-May-03	15:20	Mayor's decision: those east of I-5 can leave home with certain precautionary measures, safe for them to resume daily activities, still need to be monitored, send message that they shouldn't eat home grown vegetables, let their kids play in the dirt, and avoid dust; those west of I-5 will be relocated for 3 days. Very few people remain West of I-5 since 1200 people were evacuated last night. Use outdialer to contact them, get them out with reception points, and decon shelter run by PHSKC. Possibility of hot spots so they may need to be kept for more than 3 days		Analyst log	JOC (WA)
WA	13-May-03	15:30	Meeting between HAZMAT IC and CST commander- indication is that CST is no longer required. CST to redeploy.		Data Collector Log	RDD site
WA	13-May-03	15:34	Agriculture advisory from WA Dept. of Agriculture: The following precautionary measures are recommended in the affected areas: Do not purchase and or consume products that were stored in open-air markets after 12:10 PDT (15:10 EDT) on May 12. Do not pick or harvest fruits, vegetables or grain. Do not harvest or eat shell fish harvested after 12:10 PDT (15:10 EDT) on May 12. Do not transport uncovered agricultural products through the advisory area. Restrict pets to water sources that are covered or are from enclosed underground storage		Advisory	WA Dept. of Agriculture
WA	13-May-03	15:35	WA Disaster Field Office scheduled to open May 15		Data Collector Log	WA State EOC
IL	13-May-03	15:38	Cook County Health Department requests SNS; formal request to be made within several minutes.		Data Collector Log	Chicago EOC
IL	13-May-03	15:58	Cook County Board chairman signs joint Cook County and Chicago emergency declaration.		Data Collector Log	CCDHP
IA	13-May-03	16:00	DHS ALERT AL-03-TOPOFF2-M: "The Secretary of DHS, in consultation with the intelligence community and the Homeland Security Council, raised the national threat level to Code red nationwide as of 1600, May 13...Federal Departments and Agencies, and State and local authorities, are directed to immediately implement protective actions identified in Operation Liberty Shield..."		DHS formal memorandum	DHS
IL	13-May-03	16:10	News Release: The City of Chicago declares a State of Emergency due to Pneumonic Plague. Cites probable release sites of O'Hare Airport, United Center, and Union Station. Chicago Fire Department has determined that no further releases are suspected.		Data Collector Log	Chicago EOC
IA	13-May-03	16:19	City of Chicago requests push-pack from Strategic National Stockpile to treat outbreak of plague-like illness.		Data Collector Log	FBI SIOC
IL	13-May-03	16:20	St. Joseph's Hospital receives fax from IL Poison Center confirming <i>Y. pestis</i>		Data Collector Log	St. Joseph's, Chicago
IA	13-May-03	16:21	ICE Situation Command notified its field offices that the British Columbia Center for Disease Control had confirmed that individuals admitted to the Vancouver General Hospital on May 12 with flu-like symptoms had pneumonic plague.		Situation report from BICE HQ Reporting Center	DHS-CAT
IL	13-May-03	16:27	VNN report: Canada Health confirm cases of plague; all cases originated through Air Canada flight 783; currently tracking individuals.		Data Collector Log	IL VCC
IL	13-May-03	16:28	VNN report: rapid response team has determined three target sites for plague in Chicago - Union station, United Center and O'Hare Airport International Terminal		Detailed Incident Report	DuPage County EOC
IL	13-May-03	16:32	Fax message to Chicago EOC: IL Governor announces IDPH Laboratory confirmation of Plague		Data Collector Log	Chicago EOC
IL	13-May-03	16:33	Fax received at CCDPH - IDPH Lab confirmed plague but not confirmed terrorism. Fax sent out to provide reporting numbers for IOHNO		Data Collector Log	CCDHP
IL	13-May-03	16:35	EMS Surveillance for April 30, 2003 through May 13, 2003 showed an increase in respiratory tract symptomology with patients beginning on/about May 12 and increasing through May 13.		Data Collector Log	Chicago EOC
IL	13-May-03	16:37	DuPage County EOC received official fax from IDPH - PCR confirmation of pneumonic plague		Data Collector Log	DuPage County PH
WA	13-May-03	16:45	WA SEOC received report from Seattle EOC: confirming 20 dead and 117 injured		EOC Supervisor Log	WA State EOC
IL	13-May-03	16:50	Fax of IL Governor's emergency declaration arrived at Lake County EOC.		Data Collector Log	Lake County EOC
IA	13-May-03	16:54	Truck with Cobalt 60 that was reported missing located, cargo intact.		Data Collector Log	USDOT CMC
IA	13-May-03	17:00	SNS Operations Center has not received any requests from the IL Governor for the SNS, even though the IL Governor already announced on VNN that he'd requested SNS	It is not clear from the Situation Report when this happened, but it was no later than 17:00 EDT	Situation report #4	SNS Operations Center
IL	13-May-03	17:01	Cook County EOC: Cook County has filed and recorded a disaster declaration to ensure authorization of certain emergency procedures		SEOC Event Log	IL State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	13-May-03	17:05	Evidence collection at the RDD site: RDD site broken into 4 quadrants to establish radiological reading per quadrant. EPA will follow FBI on site, then SFD will follow - 2 teams of 2 to mark GPS coordinates.		Data Collector Log	RDD site
IL	13-May-03	17:21	Lake County EOC received fax from IL JIC stating there will be no press release referring to county disaster declarations.		Data Collector Log	Lake County EOC
IA	13-May-03	17:30	A Task Force of 250 Army National Guardsmen has been activated and will be deployed at 06:00 PDT Wednesday morning to relieve Washington State Police troopers manning road closure checkpoints.		FEMA NEOC-EST	DHS/CAT
IA	13-May-03	17:30	All air traffic into O'Hare Airport has been suspended by order of DHS, in coordination with FAA and TSA. An exception was made to accommodate the transport of shipments from the SNS.		FEMA NEOC-EST Situation report	DHS/CAT
IA	13-May-03	17:30	HHS Secretary declared a Public Health Emergency in the City of Chicago, allowing the department to provide Federal health assistance under its own authority.		FEMA NEOC-EST	DHS/CAT
WA	13-May-03	17:32	VTC discussion across EOCs regarding conflicting information over road openings: WA State Police says highways are open, but WA DOT has the authority not the police. WA DOT wants to wait until confirmation from WA DOH that it's safe.		Data Collector Log	KC EOC
WA	13-May-03	17:35	FBI reports that the Seattle port has reopened		Analyst log	JOC CMG
IL	13-May-03	17:40	Chicago EOC obtains Chicago DPH's own stockpile; clinic set up at Westside to prophylaxis Chicago DPH staff; Logistics chief to epidemiology - EOC staff have PPE.		Data Collector Log	Chicago EOC
WA	13-May-03	17:40	DMORT arrived at the incident site. A meeting with FBI, SFD HAZMAT, and DMORT ensued to determine when and where the DMORT should set up their equipment in the hot zone. It was decided that in about an hour, FBI would allow DMORT to set up after FBI was finished.		Data Collector Log	RDD site
IL	13-May-03	17:45	VNN report: HSAS raised to red for entire nation, all transport in Chicago closed, 48 hour halt to all public gathering		Data Collector Log	IDPH
IL	13-May-03	17:47	VNN report: CDC announces health alert in Illinois		Data Collector Log	IL VCC
IL	13-May-03	17:49	Signed request for NDMS and DMAT sent to FEMA Region V ROC		SEOC Event Log	IL State EOC
IL	13-May-03	17:50	VNN report: DHS Secretary announces plague in Illinois; ports, trains, and airports all closed; urge people to stay in place; Hollywood celebrities says stay in place		Data Collector Log	IL VCC
IA	13-May-03	17:50	VNN press conference with DHS Secretary, HHS Secretary, and senior FBI representative. DHS Secretary confirms plague in Illinois; announces UN invocation of UN Charter Article V, announces elevation of HSAS level to Severe (Red) nationwide for 48 hours, associates the Seattle RDD and the Illinois plague with GLODO, and says that he has asked Mayors and Governors to implement Operation Liberty Shield-like protective actions.		Data Collector Log	MCC
WA	13-May-03	17:57	Seattle EOC evacuation overview: implementing plan to let people East of I-5 to leave home with instruction on how to do so. West of I-5 we will use the same protocol as last night to evacuate all people in exclusion area. Military will be providing bus drivers for metro busses. Will use out dialer to call all local residents. People will be told to take possessions for 3 days. Leave pets with three days of food and water. People will get screened at the airport; it will be voluntary screening but we highly recommended they get screened. We will not mandate the evacuation, especially for seniors. Buses will run from 4-12 pm today. We will evacuate in an orderly manner so that no one is out standing and waiting for a bus to come along. SPD will monitor perimeter and keep out strays.		Data Collector Log	Seattle EOC
IL	13-May-03	18:00	Chicago EOC advised that SNS had been activated; surveillance staff discuss clinic staffing - decide to use existing model with plans for up to 6 distribution sites.		Data Collector Log	Chicago EOC
IL	13-May-03	18:00	IL Governor sent a letter through FEMA Region V requesting a Declaration of Major Disaster under the Stafford Act		SEOC Event Log	IL State EOC
WA	13-May-03	18:00	VNN report: DHS Secretary announcing HSAS raised to nationwide RED. PFO, who is now at the WA SEOC, just receives confirmation that HSAS raised to red.	This event occurred between 15:00 and 15:30 PDT (18:00 and 18:30 EDT)	Data Collector Log	WA State EOC
IA	13-May-03	18:00	Regional FDA director reports restriction of all food supplies within plume area	The evaluation team could not confirm when this was implemented, but it was no later than 18:00 EDT	DHS CAT Briefing on the Federal Response to Seattle RDD	DHS-CAT
WA	13-May-03	18:04	USAR team arriving now and will be operational at 20:00. Another notional team will be arriving at 08:00.		Data Collector Log	RDD site
WA	13-May-03	18:10	Seattle EOC gradually shrinking contaminated zone based on new "analytic information"		Data Collector Log	KC EOC
WA	13-May-03	18:17	KC EOC policy room wants a copy of that press release - we want confirmation before " we roll that hand grenade out into the EOC".		Data Collector Log	KC EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	13-May-03	18:20	Seattle EOC Policy room: People come in all alarmed because DHS wants to go to Red nationwide. No one knows why but that requires Americans to stay home for 48 hours. The Mayor was not asked about this and this goes against his plan to return to normalcy. Conference in EOC Directions office on about statement. Why is DHS making this statement without contacting state county or city top officials? Recommendation is that we treat this as an unconfirmed rumor and get them (DHS) to back off.	This event occurred between 15:20 and 15:35 PDT (18:20 and 18:35 EDT)	Data Collector Log	Seattle EOC
WA	13-May-03	18:30	FEMA Region X ROC deputy director - directing staff to activate their "RED" plans and procedures		Data Collector Log	FEMA Region X ROC
WA	13-May-03	18:30	WA EMD Director requests guidance from DHS Secretary on steps to take when HSAS raised to RED. We need hard copy of recommended restrictions form DHS.		EOC Supervisor Log	WA State EOC
WA	13-May-03	18:31	WA DOH determines that I-5 can be reopened; WA DOH passes information to WA DOT		Data Collector Log	WA State EOC
IA	13-May-03	18:40	SNS Operations Center received request for SNS and approval to deploy 1 push-pack to Chicago	Follow-up calls by analyst confirm the deployment was approved by FEMA Director, EP&R, DHS, in conference with CDC Deputy Chief of Staff	Situation Report	SNS Operations Center
IA	13-May-03	18:58	HHS/SCC conference call - key discussion points: Prussian Blue availability and the lack of specific guidance on large-scale use; primarily used with people exposed after they are decontaminated. Difficulty of assessing internal exposure within individuals injured in the blast. Public Health officials recommend that travellers be alerted and a "fever watch" instituted for those people potentially exposed to plague. Chicago asked non-essential employees to stay home. That might impact availability of healthcare personnel.		Data Collector Log	HHS
IA	13-May-03	19:00	Memorandum for the President: Request for an Emergency Declaration for the State of Illinois From: Under Secretary, EP&R (Michael D. Brown). Event: On May 12,2003 Governor Blagojevich requested a major disaster declaration due to an outbreak of Pneumonic Plague in the City of Chicago (Cook County) and four surrounding counties. The Governor does not specify a specific type of assistance but rather requests supplemental Federal assistance to preserve lives and property and protect public peace, health and safety.		Data Collector Log	CDC EOC Atlanta
IL	13-May-03	19:18	Director of Chicago OEMC briefing: Press release provided declaring State of Emergency: Closing schools, O'Hare and Midway Airports are closed by DHS Secretary. SNS estimated to be arriving at 10:00 CDT (11:00 EDT) on May 14 at O'Hare Airport with 1 million doses for first responders and those first affected - this is enough meds to treat a single person for a week and is enough for Chicago and surrounding counties; there will be a lag period for breaking down SNS and distribution - hopefully, will begin the distribution on May 15.		Data Collector Log	Chicago EOC
WA	13-May-03	19:20	WA SEOC reviewed air space closures: because of RED alert status, decision was made that restrictions would remain in place		Data Collector Log	WA State EOC
WA	13-May-03	19:20	Road status: I-5 reopened, but not exit to downtown Seattle or West side of I-5; I-90, SR 520, and West Seattle bridge all reopened; SR 99 closed until sampling is completed, results expected in 2 hours.		Data Collector Log	WA State EOC
IL	13-May-03	19:25	Chicago EOC reports EMS volume increased by 10%; 6 ready reserve ambulances placed in service; private ambulance contractor notified for possible activation; 15 spare ambulances will require waiver from IDPH to place in service.		Data Collector Log	Chicago EOC
WA	13-May-03	19:30	WA SEOC News release: Washington State Ferries will resume their full public service schedule beginning at 4:30a.m.on May 14, with some exceptions		News Release	WA State EOC
WA	13-May-03	19:42	Deputy Mayor advises Mayor of I-5 opening. Flushing has already taken place. Public message to indicate significant delays; encourage public transportation.		Data Collector Log	RDD site
WA	13-May-03	19:54	SPD SWAT arrives at suspected GLODO safe house		Data Collector Log	RDD Site
WA	13-May-03	19:55	At 1500 hours, Washington Department of Health provided preliminary lab tests. These results showed the presence of four isotopes: cesium 137, plutonium 238, plutonium 239 and americium 241. Soil samples are being forwarded to DOE for more thorough analysis.		Intelligence Summary Report	WA FBI Field Office
WA	13-May-03	19:58	SPD SWAT completes take down of suspected GLODO safe house		Data Collector Log	RDD Site
IL	13-May-03	20:00	IEMA reported Midway and O'Hare airports are closed by DHS; curious if American Red Cross will attend to needs of stranded travelers		SEOC Event Log	IL State EOC
WA	13-May-03	20:16	SPD IC states crime scene part is done so SFD is in charge.		Data Collector Log	RDD site

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	13-May-03	20:17	SFD requested mutual aid for HazMat to continue recovery operations		Data Collector Log	RDD site
WA	13-May-03	20:18	KC EOC policy room receives report that I-5 and West Seattle Bridge will reopen at 1800 tonight.		Data Collector Log	KC EOC
IA	13-May-03	21:05	The NRC reported yesterday evening at approximately 1800 (MST) the Palo Verde Generating Station received an anonymous bomb threat against the facility. The caller said the environment has been damaged enough through radiation poisoning and he and Allah will take revenge. The caller did not claim to be part of any terrorist organization and there is no evidence to corroborate the threat.		Data Collector Log	HHS
WA	13-May-03	21:14	Unified command meeting: 1) FBI advised their assets are pulled out. 2) FEMA advised they are in charge under FBI; FEMA has given command to locals - SPD and SFD have unified command now together.		Data Collector Log	RDD site
WA	13-May-03	22:40	King County Executive in keeping with DHS Secretary request for all people to remain at home made the following announcements regarding County services effective through Thursday, May 15: Essential County services will be maintained such as public health and safety, however, only essential personnel will be on duty; The District and Superior Court Judges have suspended all scheduled hearings at all court locations. Scheduled jurors should not report until further notice; The Regional Justice Center in Kent Jail Division will continue as it has this week; Metro Transit will be operating on a modified holiday schedule. The Downtown Seattle Transit Tunnel will be closed; All King County transfer facilities and Cedar Hills landfill will be closed until further notice. Residents that have garbage should bag their garbage put in a secure place until service resumes; King County is asking all essential personnel to report for work. King County employees should check with their supervisors; Updates on this and other information can be found on our Web site at www.metrokc.gov or by listening to local news.		Press Release	KC IC
IA	13-May-03	22:50	SIOC: recommend that Chicago should stand-up a JOC		Data Collector Log	FBI SIOC
IA	13-May-03	22:50	HHS convenes Emergency Policy Support Group.		Data Collector Log	FBI SIOC
WA	13-May-03	23:22	WA SEOC received call from Seattle EOC that field play concluded		Data Collector Log	WA State EOC
WA	14-May-03	0:25	Consider this a formal request from the State of Washington: City of Seattle is requesting release of prepositioned equipment package being held at Boeing Field by DHS.		Email	WA State EOC
IA	14-May-03	2:55	HS Center report from FEMA EST: The FEMA EST is requesting guidance as to what is the expectations of the States under treat condition "Red."	Period Covered: 0200 May 14, 2003 to 1300 May 14, 2003 PDT	Region X ROC input to EP&R situation report	DHS-CAT
IA	14-May-03	8:10	FEMA conference call with Regions to discuss numerous State inquiries regarding SNS push packages.	Period covered: 0700 hours EDT May 13 to 1730 EDT May 15	EST Situation Report	FEMA NEOC-EST
IL	14-May-03	8:18	DuPage County DPH Director authorized the release of antibiotics to his staff.		Data Collector Log	DuPage Co. Health
IA	14-May-03	8:23	INJECT: DOT FRA activates the Regional FRA COOP plan in Chicago		Data Collector Log	DOT CMC
IL	14-May-03	8:25	Phone conversation between IOHNO and IDPH; per IL Gov's press release, United Center and Union Station was not listed to close down - IDPH recommends those venues be closed until FBI/Law enforcement determines terrorist related and marks those venues as crime scene.		Data Collector Log	IOHNO
IL	14-May-03	8:35	DuPage County DPH morning briefing: at 15:25 CDT (16:25 EDT) on May 13, IDPH released information about plague, requested the SNS, and authorized distribution of antibiotics to those who may have been exposed; at 17:42 CDT (18:42 EDT) on May 13, IDPH reported plague confirmed; people who were at United Center, Union Station or O'Hare on May 10 or later may be exposed and recommended for prophylaxis; a local declaration is no longer needed as the state declaration is sufficient.		Data Collector Log	DuPage Co Health
IL	14-May-03	8:40	DuPage County DPH directed the staff to prepare for the delivery of the SNS.		Data Collector Log	DuPage Co. Health
IA	14-May-03	8:45	TSA and FRA discuss potential rail shutdown. FRA clarifies that STB is the only authority that can shut down rail.		Data Collector Log	VA Central Office
IL	14-May-03	9:00	ARC agrees to support stranded travelers with mass care, health services, and mental health.		Data Collector Log	ARC - Chicago HQ
IL	14-May-03	9:05	DHS Secretary provides update on VNN: terrorist attack, plague confirmed, bioterrorism event.		Data Collector Log	IOHNO
IA	14-May-03	9:11	MST tasked to come up with recommendations for disposing of contaminated bodies. CDC working with MST to do this.		Data Collector Log	DOT CMC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	9:17	IDPH Director authorized distribution of prophylaxis to first responders.		Detailed Incident Report	DuPage County EOC
IL	14-May-03	9:30	Chicago DPH Situation report: NDMS requested.		Situation report	Chicago DPH
IL	14-May-03	9:30	Chicago DPH Situation Report. O'Hare and Midway airports and Union Station in Chicago have been closed by the U.S. Department of Homeland Security (DHS)		Situation report	Chicago DPH
IL	14-May-03	9:30	Chicago DPH Situation report: IL Governor has recommended that non-essential workers in the affected area stay home. Schools in Cook, DuPage, Kane and Lake counties have been closed. DHS has recommended that all non-essential large public gatherings be cancelled.		Situation report	Chicago DPH
IL	14-May-03	9:30	VNN report: DHS Secretary has closed O'Hare, Midway airports and Union Station		Data Collector Log	Springfield IDPH
IA	14-May-03	9:45	Department of Veterans Affairs update to HS Center: VA has informed all facilities of increase in National Threat Level to RED and initiated the implementation of level red protective measures for all VA facilities. In response to alert level RED, VA's pre-COOP team is on alert to deploy (notionally) to VA's primary COOP site at 15:00 this Wednesday afternoon. A Secretarial successor will be on-site. 20 Plague patients presented to VA Medical Center Hine, Illinois; 10 patients were admitted to isolation beds and 10 died. VA provided the White House and HHS inventory of pharmaceutical assets, appropriate for use in the treatment and management of Plague, located in the Chicago area.		Data Collector Log	DHHS-SCC
IL	14-May-03	9:48	DuPage County DPH notified DuPage County EOC to tell first responders to come for prophylaxis.		Data Collector Log	DuPage Co. Health
IL	14-May-03	9:57	IDPH requesting: 5 IL DOT vehicles and drivers; 5 IL Corrections vehicles and drivers; 27 IL State policemen and 6 cars; and 40 IL National Guard members to be at the FedEx Terminal at O'Hare Airport by 10:00 CDT (11:00 EDT).		SEOC Event Log	IL State EOC
IL	14-May-03	10:00	La Grange Hospital received fax from IL Governor warning employees of non-essential businesses to stay home until further notice.		Data Collector Log	LaGrange
IL	14-May-03	10:00	City of Chicago shut down all passenger transportation in and out of Chicago, including airports.		Data Collector Log	FEMA Region V ROC
IL	14-May-03	10:03	IL Governor signs "Executive Order" considering this to be a possible bioterrorist, suspended HIPAA and Blood Banks...allow state to share communicable disease information with law enforcement; suspended licensing act so that physicians can practice in places where they are not licensed...temporarily suspend legal constraints on other professionals so that others can dispense medications, and disseminate at other places other than pharmacies (distribution and administration of antibiotics).		Data Collector Log	Lake County EOC
IA	14-May-03	10:05	The President (notional) granted an emergency declaration (FEMA-4322-EM-IL) to Illinois May 14, to address the health crisis in the Chicago area. The declaration covers Cook, DuPage, Kane and Lake Counties. An FCO was appointed.	Note: A Major Disaster Declaration was requested by the IL Governor, but an Emergency Declaration was granted.	Declaration	DHS/CAT
IA	14-May-03	10:06	The White House, FBI and DHS are looking to HHS for leadership in crafting public health message concerning events in Chicago and Seattle.		Data Collector Log	VA Central Office
IA	14-May-03	10:06	CDC called SIOC: Deployed SNS push pack and re-deployed teams		Data Collector Log	VA Central Office
IA	14-May-03	10:06	FPS has deployed police officers to support CDC operations in Chicago to augment security operations since deaths and plague cases are increasing drastically today.		Data Collector Log	VA Central Office
IL	14-May-03	10:14	IL SEOC reports that DuPage County has begun the prophylactic distribution process.		SEOC Event Log	IL State EOC
IL	14-May-03	10:16	To Lake County Government Employees from County Board Chairman: Lake County joined several other government entities "in declaring a disaster situation in particular jurisdictions... as part of the disaster declaration; Lake County Government offices will be closed beginning tomorrow, Wednesday, May 14th except for those personnel required for the continuation of critical government functions. This is in concurrence with US DHS Secretary's advice that people "take a snow day" in order to remain isolated and safe in their homes."		Email	Lake County EOC
IL	14-May-03	10:30	CCDPH notified of meeting earlier this morning between Cook County Chief Counsel and IL Governor: considering this to be a possible bioterrorist, suspended HIPAA and Blood Banks...allow state to share communicable disease information with law enforcements; suspended licensing act so that physicians can practice in places where they are not licensed...temporarily suspend legal constraints on other professionals so that others can dispense medications, and disseminate at other places other than pharmacies (distribution and administration of antibiotics)...		CCDPH Player Log	Cook County DPH
IL	14-May-03	10:30	Press conference at IL JIC: confirms release of plague at United Center, O'Hare and Union Station - only at these three sites. Governor actions: requests SNS deployment, State of Emergency in IL, deployment of WMD team and IMERT Team to increase security.		EOC Log	Lake County EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	10:30	Lake County EOC report to Lake County Health Department Incident Command Post: DuPage County beginning prophylaxis of first responders with DuPage County Department of Health stockpile.		Email	Lake County EOC
IL	14-May-03	10:35	IOHNO requests Deoxycycline, Ciprofloxacin, surgical masks, and ventilators from VMI		Data Collector Log	IOHNO
WA	14-May-03	11:00	FEMA Region X ROC transferring management of recovery operations to DFO tomorrow at 12:00 and will handle RDD-related issues		Data Collector Log	HHS Region X REOC
IL	14-May-03	11:03	IDPH Lab receives IL executive orders suspending privacy rights, etc...		Data Collector Log	IDPH lab
IL	14-May-03	11:03	FEMA Region V ROC reports to IL SEOC that 18 hospitals in Chicago & suburbs are at maximum capacity. FEMA needs to know the names of the hospitals to support. Regarding the NDMS request - please report information to FEMA liaison at IL SEOC for transmittal back to FEMA Region V ROC		SEOC Event Log	IL State EOC
IL	14-May-03	11:08	Chicago EOC confirmed: O'Hare airport is closed; midway airport is closed; Union station and all railways are shut down; all bus systems in and out of the city are suspended.		Detailed Incident Report	DuPage County EOC
IL	14-May-03	11:10	IDPH has established an information hotline 1-877 867 6332		SEOC Event Log	IL State EOC
WA	14-May-03	11:20	Based on new information, SeaTac is outside the TFR; air traffic controllers can reroute traffic to avoid waivers		Data Collector Log	FEMA Region X ROC
IL	14-May-03	11:25	IL DOT liaison at O'Hare FedEx terminal reported to IL SEOC that SNS has arrived		SEOC Event Log	IL State EOC
IL	14-May-03	11:30	Chicago EOC received clarification of Chicago Transit Authority service: service continues within city limits; no service to suburbs or airports.		Data Collector Log	Chicago EOC
WA	14-May-03	11:30	NMRT arrived at VA Hospital (WA)		Data Collector Log	VA Hospital (WA)
IL	14-May-03	11:32	CCSEMA received fax from DHS/FEMA - IL granted Federal Emergency Declaration		Message & Event Log	CCSEMA
IL	14-May-03	11:33	Vancouver officials acknowledged that their plague victims came from Air Canada flight #783 on May 10 from Chicago.		Agency Log	Chicago DPH
IL	14-May-03	11:35	CDC has arrived at IOHNO to assist with SNS.		Data Collector Log	IOHNO
IL	14-May-03	11:40	IL SEOC advised that the SWMDTs are attempting to rescue a security guard who has been shot behind building 32 at Nalco Chemical Plant		SEOC Event Log	IL State EOC
IL	14-May-03	11:45	Cook County EOC receives CDC Health Alert: recommends prophylaxis and protection of workers at suspected plague release sites. Three sites in the Chicago area have been identified as likely exposure sites based on the initial epidemiologic information. The sites identified are the United Center, Union Station and O'Hare International Airport. Persons who have been in these venues for the period May 10 through May 13 are advised to seek antibiotic prophylaxis.		HAN	Cook County EOC
IL	14-May-03	11:45	IDPH and CDC liaisons at IOHNO note that Federal SNS assets are being released without a federal disaster declaration.		Data Collector Log	IOHNO
IL	14-May-03	11:47	SNS being loaded onto semis for movement; scheduled for actual move at 12:30 CDT (13:30 EDT)		Command Post Log	Nalco Chemical Plant Bldg 26

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	11:56	CDC formally signs over entire SNS package.		Data Collector Log	SNS Reception Site at O'Hare International Airport
IL	14-May-03	11:56	IDPH Lab hears about shooting in at Nalco Chemical Plant.		Data Collector Log	IDPH Lab
IL	14-May-03	12:00	Ingalls Hospital received fax from IDPH: presumptive plague exposure at Chicago Union Station and O'Hare Airport International Terminal limited to May 10.		Data Collector Log	Ingalls
IL	14-May-03	12:03	VNN clarifies plague cases and deaths in Chicago: 333 dead and 1,676 suspected cases. Presidential declaration made, FBI confirms terrorist attack		Data Collector Log	ARC - Chicago HQ
IL	14-May-03	12:15	FEMA Region V ROC reported to IL SEOC: at 10:05 CDT (11:05 EDT), the President signed an Emergency Declaration for IL ; as of 10:55 CDT (11:55 EDT), FEMA Region V ROC did not have a copy of declaration nor assigned disaster number; not known if declaration applies to entire State or just specific counties.		SEOC Event Log	IL State EOC
IL	14-May-03	12:15	Security guard has been rescued and transported to local hospital; investigations to conduct interview of guard.		Command Post Log	Nalco Chemical Plant Bldg 30
IA	14-May-03	12:25	FEMA and TSA discuss obtaining waivers for emergency flights through restricted airspace.		Data Collector Log	FEMA EST
IL	14-May-03	12:30	Lake County EOC learns that IL granted Federal Emergency Declaration		Agency Log	Lake County EOC
WA	14-May-03	12:30	King County update regarding Airports: Seatac is open and on normal operations. FAA restrictions: TFR reduced to an elevation of 2,000 ft. King County Airport open Renton and Paine Field Airports open.		Coordination Briefing	KC EOC
IL	14-May-03	12:35	DMORT has been activated - they will deploy to Hines VA Hospital (IL); Satellite clinic site requested to be opened at Hines VA		Incident Report	Cook County EOC
IL	14-May-03	12:43	DuPage County EOC requested all county emergency management agencies, City of Chicago, IL JOC, and IL SEOC to join a conference call at 13:00 CDT (14:00 EDT) to discuss SNS prophylaxis strategy. It is suggested that the county board chair/administrator sit in if possible.		Email	Lake County EOC
IL	14-May-03	12:50	IDPH now has 30K + 30K doses available for Chicago: Public messages will be clear about risk groups and not to abuse system. Those who have been in contact with known cases (family members, etc) to be issued coupons for identification. 300K doses to be delivered by per day.		Data Collector Log	Chicago EOC
IL	14-May-03	12:50	Press Release that Plague outbreak linked to three Chicago area locations from May 10: International Terminal at O'Hare Airport, United Center, and Union Station.		EOC Log	Lake County EOC
WA	14-May-03	13:00	WA SEOC received casualty status from Seattle EOC: 20 Confirmed Dead; 130 Injured		Situation Report	WA State EOC
IA	14-May-03	13:08	FPS has contacted CDC in Atlanta to advise that Emergency Response Team is on stand-by and available to support their security guards in the event that there are protests or attempts to get into their facility for plague antidotes.		Data Collector Log	DOT CMC
IL	14-May-03	13:10	CCSEMA received call from Cook County Medical Examiner (CCME): report that Chicago Police requested and received a deployment of 8,000 National Guard troops who can assist with mortuary services. CCME's office has requested 200 of these troops to be dedicated to Cook County mortuary operations.		Message & Event Log	CCSEMA

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	13:25	VNN report: DHS Secretary instructing all citizens working at any of the (or was at any of the) target sites should go immediately to a medical facility for medications. DuPage County Emergency Management Agency response is to 1. Call hospitals. 2. Law enforcement.		Data Collector Log	DuPage County EOC
IL	14-May-03	13:25	DuPage County Commissioner recommends immediate PIO release - "Ignore" the FEDS, listen to local officers. Conflict between DHS Secretary's exact comments and what had already been released to Media.		Data Collector Log	DuPage County EOC
IL	14-May-03	13:30	SNS was received at 12:30 by Cook County Sheriff's office; contains only 5% of the shipment we were suppose to receive.		Agency Log	Cook County DPH
IL	14-May-03	13:30	Request came into IL SEOC from EPA to perform monitoring (BIOWATCH) at Union Station, O'Hare field and United Center. EPA is moving some portable sampling devices from Wisconsin to Des Plaines (IEPA's Regional Office). Target to have the additional sampling locations operational is 14:30 CDT (15:30 EDT)		SEOC Event Log	IL State EOC
IL	14-May-03	13:30	VNN report: GLODO claims responsibility for terrorist attack of plague in Chicago. They say "their terror is now our terror."		SEOC Event Log	IL State EOC
IL	14-May-03	13:36	Chicago DPH closing major assemblies and events in Chicago.		CDPH	Chicago DPH
IA	14-May-03	13:59	Cook County has requested VA to supply 25 refrigerated trucks to serve as morgue		Data Collector Log	VACO
IL	14-May-03	14:02	Open conference call between IDPH and the 5 effected counties. Issues discussed involved number of doses and the number of cases which could be addressed. Concern about unexposed people coming to distribution centers to get medications and getting exposed at the site. Media problem - need to get people to understand that if they are not symptomatic, were not at one of the three sites, and were not exposed, they don't need to take medications. Medications are not an endless supply and Illinois may only be the 1st state to be hit.	Earlier request for this meeting suggested top officials be present, they don't appear to have attended	Data Collector Log	Cook County EOC
IL	14-May-03	14:24	Press release: HHS Sends Medical Staff To Chicago		Email	Lake County EOC
IL	14-May-03	14:28	Joint Media Release: HEALTH OFFICIALS ANNOUNCE LOCATIONS OF PLAGUE RELEASE. The office of IL Governor announced this morning three locations where plague was released by terrorists last Saturday, May 10. The locations are Union Station in downtown Chicago, the International Terminal of O'Hare airport and United Center on the city's west side. No other sites have been identified... Those who were at one of the sites on Saturday should receive antibiotics to prevent the development of illness. Those in close contact with someone exhibiting symptoms should also receive antibiotics.		Email	Lake County EOC
IL	14-May-03	14:40	Cook County EOC reports: CCDPH personnel starting to offload and break down SNS; CCSEMA duty officer onsite at Bridgeview dispensing site.		Email	Lake County EOC
IL	13-May-03	14:59	Good Samaritan Hospital ER received call from Loyola Hospital to activate Phase II of IL Emergency Medical Disaster Plan		Data Collector Log	Good Samaritan Hospital
IL	14-May-03	15:00	IL Department of Natural Resources (DNR) closing IL state parks		SEOC Event Log	IL State EOC
WA	14-May-03	15:05	USCG lifted No Sail Order in WA		Agency Log	KC EOC
IL	14-May-03	15:20	Chicago EOC received EmNet Emergency Message: the SNS have been received, broken down and loaded for delivery to the dispensing site.		EmNet Emergency Message	Chicago DPH
IL	14-May-03	15:25	Kane County would like wait to release information about SNS distribution until the morning of May 15 - only 1 distribution site in Kane County; fear that an earlier release would not be beneficial. There appears to be a consensus that information will be released this evening stating that distribution sites will be made public on the morning of the 15th.		Data Collector Log	Kane County DPH
IL	14-May-03	15:35	FEMA provided information to IL SEOC: Presidential Emergency Declaration applies to 4 affected counties in IL: Cook (including Chicago), DuPage, Kane and Lake		SEOC Event Log	IL State EOC
IL	14-May-03	15:45	Call from CCSEMA Staff & Duty Officer - SNS arrived at Bridgeview dispensing site		Message & Event Log	CCSEMA
WA	14-May-03	16:02	Burlington Northern Santa Fe report of a possible complete shutdown of Amtrak & Sounder passenger Service. Some trains in the "hot zone" and won't know the extensive assessment of the contamination for weeks or months. Freight is being routed around exclusion area from Ballard to Tukwila. Potential economic impact discussed		Situation Report	KC EOC
IL	14-May-03	16:10	Kane County has received its allotment of the SNS		SEOC Event Log	IL State EOC
IL	14-May-03	16:10	Lake County EOC to lake County Health Department Incident Command Post concerning SNS eligibility: Shortage of medications through SNS (IL Pharmaceutical Stockpile going to hospitals); need recommendations as to how limited supply would be used. REPLY: Vendor Managed Inventory implemented - number of antibiotics is no longer an issue; however, mass prophylaxis - to any and all - is being discussed by health departments in region.		Email	Lake County EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	16:15	City of Chicago expecting SNS to arrive at 14:45 CDT (15:45 EDT)		Data Collector Log	Chicago FD Training Academy
IL	14-May-03	16:15	ARC of Greater Chicago CEO on VNN: confirms blood supply in Chicago is safe - no need for new donations. Also, ARC of Greater Chicago Disaster Welfare Information System lines are open for separated family members. Red Cross health and mental health workers are at hospitals, airports, and rail stations to support stranded passengers.		Data Collector Log	ARC - Chicago HQ
IL	14-May-03	16:22	Multiple hospitals indicate that there are no medical beds available. Concerns regarding staffing. Hospitals have gone to lock down mode due to increased crowds.		Detailed Incident Report	DuPage County EOC
IL	14-May-03	16:25	Chicago Fire Department Chief: 120 boxes of inbound SNS will stay at Fire Department; the rest will go with City Department of Health to distribution site.		Data Collector Log	Chicago FD Training Academy
WA	14-May-03	16:25	WA Dept. of Agriculture established food control areas and road access checkpoints for agricultural products in potentially affected counties to prevent people consuming contaminated fresh food and milk products.	Don't know if this is the final food control plan	Talking points for TOPOFF 2. Food and Safety Control	WA State EOC
WA	14-May-03	16:32	WA DOH realizing exclusionary zone probably should have been expanded 2 days ago. Concerned about wind increase and dispersment of the elements. WA DOH very concerned about Seattle's plan to further shrink the exclusion zone		Data Collector Log	WA State EOC
IL	14-May-03	16:35	Chicago OEMC requested an additional 4000 IL National Guard troops		SEOC Event Log	IL State EOC
IL	14-May-03	16:55	IL officials concerned that Presidential Emergency Declaration vice Major Disaster Declaration results in loss of (a) crisis counseling and (b) disaster unemployment aid; Department of Justice may be able to fill gap with victim fund.		Data Collector Log	FEMA Region V ROC
IL	14-May-03	16:56	SNS arrived at Lake County drop-off site.		Data Collector Log	Lake County EOC
IL	14-May-03	17:31	Chicago EOC reports that SNS arrived at the Lake County Reception site at 14:50 CDT (15:50 EDT). It has been broken down and distribution to first responders has commenced as of 16:00 CDT (17:00 EDT).	Similar report reached IL SEOC at 16:32 CDT (17:32 EDT)	Emnet Emergency Message	Chicago DPH
IL	14-May-03	17:39	Chicago EOC developing a plan for all city employees to receive training and education on the risks and hazards of the current outbreak. Information being developed by all agencies, with the Chicago DPH taking the lead. Information will go out to all agencies and PIOs from affected groups. Looking at a coordinated program for union and non-union employees. Developing training video; copies to all represented departments and agencies. Training video on Channel 23 - the municipal channel; press releases already on City's internet site; this training video will be on this internet channel too. Chicago OEMC PIOs putting together radio and TV Public Service Announcements - 30 seconds. Chicago Alternative Police Strategies (CAPs) distribution program - to contact block clubs; other languages to reach diverse populations of Chicago: Polish, Spanish, Arabic, English. Leadership by example - management will lead union employees as they enter areas considered to be "at risk."		Data Collector Log	Chicago EOC
IL	14-May-03	17:40	CCSEMA received call from Cook County Sheriff's Command Center: first responders have started to receive the medication at Bridgeview dispensing site		Message & Event Log	CCSEMA
IL	14-May-03	17:40	Cook County EOC Press Release: FOR IMMEDIATE RELEASE - GOVERNOR ANNOUNCES RECEIPT, BREAKDOWN AND DISTRIBUTION OF SNS		Press Release	Cook County EOC
WA	14-May-03	17:51	WA DOH just receives fax with radiological data that arrived at SEOC yesterday. Clear that the readings exceed boundary of City's exclusionary area.		Data Collector Log	WA State EOC
IL	14-May-03	18:00	CFD Fire Academy Commander reports to Chicago EOC: they have notified outside agencies to begin picking up SNS prophylactic meds at Fire Academy; Chicago Police Dept.'s picked up 5500 doses; Chicago DPH will release rest as necessary.		Data Collector Log	Chicago EOC
IL	14-May-03	18:15	Lake County EOC: IL Governor recommends public and employees of non-essential businesses to stay home until further notice; Chicago area - target of terrorist attack.		Agency Log	Lake County EOC
IL	14-May-03	18:22	Chicago EOC: SNS arrived; holding on to drugs until 08:00 tomorrow morning as was decided with the other counties.		Data Collector Log	Chicago EOC
IL	14-May-03	18:42	IL SEOC briefing: Chicago distribution centers will operate 8:00am-4:00pm tomorrow / Cook and Lake Counties will open at 8:00am - closing time not known; DuPage & Kane Counties - no information		SEOC Event Log	IL State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	18:50	SNS Reception Site reported to the IL JOC that the SNS relay had been delivered and the detail secured. The Command Post at O'Hare has been sealed and closed. The relay was completed without incident.		SEOC Event Log	IL State EOC
IA	14-May-03	18:50	Defense Coordinating Officers deployed to Seattle and Chicago	This was reported between 18:50 and 19:20 EDT	Data Collector Log	VA Central Office
IL	14-May-03	19:03	Chicago DPH received EmNet emergency message: DuPage County has begun prophylactic distribution procedures		EmNet Emergency Message	Chicago DPH
WA	14-May-03	20:00	WA SEOC reports in SITREP that WA National Guard will activate 2 additional task forces (a total of 500 soldiers) to support law enforcement agencies.		Situation Report	WA State EOC
IL	14-May-03	20:26	IL SEOC received EmNet emergency message: Cook County Dispensing site located in Bridgeview has closed as of 19:00 CDT (20:00 EDT). The first responders have been given the medications. The dispensing site will re-open at 08:00 CDT (09:00 EDT) on May 15 for dispensing to the public.		SEOC Event Log	IL State EOC
IL	14-May-03	20:37	IL SEOC provided the following inject: Vendor Managed Inventory from the SNS arrived in IL. The State of IL has begun distribution of antibiotics and medical supplies. SNS requests made by local health departments and hospitals will continue to be filled for the length of the event		SEOC Event Log	IL State EOC
IL	14-May-03	20:38	IL SEOC report: VMI has arrived at O'Hare. State distribution staff are breaking down and will distribute to local jurisdictions as previously reported		SEOC Event Log	IL State EOC
IL	14-May-03	21:30	SNS Distribution Process: Chicago expected 60,000 doses. SNS broken down at CFA (Chicago fire Academy): only 5,500 sent over.		Data Collector Log	Chicago EOC
IL	14-May-03	22:22	IL SEOC receives report from IL State Police: Unified Command Post advised of suspect in custody who provided following info: (1) Member of Free America Group; (2) No hostages in building; (3) There is lab equipment in men's room of Nalco Chemical Bldg. 32; (4) A rail car on west side of Bldg. 32 has explosives; (5) A tank in Bldg. 32 on north side has explosives; (6) A tractor/trailer parked outside Bldg. 32 with unknown chemicals; (7) There are several booby traps in Bldg. 32		SEOC Event Log	IL State EOC
IL	14-May-03	23:15	IL SEOC sent fax to 4 counties and Chicago that VMI has been received. Being broken down at O'Hare airport. Available upon request to each county and Chicago.		SEOC Event Log	IL State EOC
IL	14-May-03	23:39	Tactical Response Team (TRT) made entry into Nalco Chemical building #32 and are inside		Command Post Log	Nalco Chemical Plant Bldg 146
IL	14-May-03	23:45	TRT advised 3 males and 1 female in custody		Command Post Log	NALCO chem plant bldg 9
IL	15-May-03	0:08	Report to IL SEOC: TRT entered Nalco Chemical Building; 3 male, 1 female in custody. 4 subjects and 16 TRT being contaminated. Preparing to sweep for explosives. Investigating personnel waiting to interrogate.		SEOC Event Log	IL State EOC
IA	15-May-03	0:15	CBP Update: -Holding all containers from high-risk countries (Pinkland, Orangeland, and Redland) transiting through CSI participating countries and increase examination scrutiny up to 100% of containers destined for the US -Deployed Border Patrol Tactical Unit (BORTAC) units (12 members each) to Seattle and to a staging location near Chicago; CBP will coordinate with the US Marshals Service for J-PATS flights to provide air Transportation Security Administration -Passenger Manifests for all international flights departing O'Hare since 11 May shared with State and Foreign LE counterparts to locate potential plague cases		Secretary's Morning Summary Operational Response	DHS HSCenter
IA	15-May-03	0:15	Transportation: -Nationwide; Liberty Shield level 1 and 2 transportation restrictions. -Nationwide: All passenger rail stopped, TSA authority questioned by Federal Railroad Administration -Port of Chicago at MarSec 3 - commercial vessel crews restricted to vessels -Chicago: Second day of transportation restrictions in Metro area		Secretary's Morning Summary Operational Response	DHS HSCenter
IA	15-May-03	0:15	EP&R Update: -EP&R Experts on scene in Chicago: 13 NDMS specialists, 14 EPI intelligence service officers, CCRF: 150 Nurses, 25 Physicians (arrive 15 May), transport of 175 Medical Personnel to Chicago -EP&R Assets in route: 2 DMATS, 1 DMORT, 50 respiratory Technicians		Secretary's Morning Summary Operational Response	DHS HSCenter
IL	15-May-03	0:20	IL State Police: 1 male subject with sucking chest wound being transported to Christ Hospital, Oak Lawn. 2 investigators in ambulance, uniformed officer also being sent to hospital for security. Other 3 subjects uninjured, being transported to Bedford Park PD, FBI en route. No injuries to ISP. Chemical still unknown. Decon by Bedford Park Fire department.		SEOC Event Log	IL State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	15-May-03	0:35	IL State Police meeting with FBI. They are in agreement with bringing in team from US EPA		SEOC Event Log	IL State EOC
IL	15-May-03	1:32	Chicago Police Dept. begins distribution of prophylaxis to Police department		Data Collector Log	Chicago EOC
IL	15-May-03	1:41	IL SEOC update on Nalco Chemical Building: ISP reports Bomb Squad has located two explosive devices. Device #1 is attached to rail tank car containing hydrazine and is a briefcase. Device #2 is attached to a rail tank car containing dichlorobutene and is equipped with a motion sensor. Working with Chicago Fire/Police, Bedford Park Fire/Police, IEMA & IMERT to extend evacuation area to 1/2 mile		SEOC Event Log	IL State EOC
IA	15-May-03	5:45	FEMA EST Situation Update: To limit the potential for spreading the disease, the transportation centers of O'Hare Airport, Midway Airport, Union Station and the Port of Chicago have been closed.		Region X ROC Input to EP&R situation report	DHS/HSCenter
IA	15-May-03	7:00	FEMA EST Situation Update: DHS reports transportation restrictions in Seattle have been lifted, except the nuclear power plant.		Data Collector Log	FEMA EST
IL	15-May-03	8:30	Joint media release: Dispensing Site Locations for Antibiotics Announced. Health Depts will provide antibiotics for all those affected by plague outbreak. Clinics: Chicago, 100 W. Virginia Street; Cook County, 120 St. James Place, Bolingbrook, DuPage County: 34 Marvin Gardens, Wheaton, Kane County: 46 Park Place, Aurora, Lake County: 75 Boardwalk, Wauconda		Joint Media Release	Cook County EOC
IA	15-May-03	8:57	VNN report: 103 Deaths in Canada - 54 Vancouver, 21 Toronto, 22 Ottawa, 1 Edmonton, 2 cases Montreal & Winnipeg		Situation report FEMA NEOC-EST	DHS-CAT
IA	15-May-03	8:57	FEMA EST Situation Update: FTA is working with WA DOH to have Ferries and terminals at Seattle, Bremerton, and Bainbridge decontaminated.		Situation report FEMA NEOC-EST	DHS-CAT
IL	15-May-03	9:00	Chicago EOC announced prophylaxis sites open to the public.		Data Collector Log	Chicago EOC
IL	15-May-03	9:00	VNN news notifying the public of dispensing of meds: Symptomatic persons are to seek medical attention. Persons who were at the 3 sites or those persons exposed to people who were at the 3 sites are to go to the facility to get meds.		Data Collector Log	Cook County EOC
IA	15-May-03	9:57	VNN report: Bio lab found in Bedford, IL		Data Collector Log	DOT CMC
IL	15-May-03	10:02	Kane County DPH reports SNS arrives and brought down for distribution		Data Collector Log	IMSA - Kane DPH
IL	15-May-03	10:03	IL SEOC reports: Lake County began dispensing operations at 8:32 CDT (9:32 EDT)		SEOC Event Log	IL State EOC
IL	15-May-03	10:06	IL SEOC reports: Du Page County began dispensing SNS at 08:00 CDT (09:00 EDT)		SEOC Event Log	IL State EOC
IL	15-May-03	10:20	ISP and FBI confirm backpacks with aerosol cans were located at airport and were used for distributing of plague.		SEOC Event Log	IL State EOC
IL	15-May-03	10:32	IL SEOC received EmNet Emergency message from IL JOC: FEMA representative indicated that there has been a toll free # set-up for financial assistance and for hearing impaired. Also reimbursement is available to local and state agencies for eligible costs of equipment, contracts and personnel overtime related to emergency services in dealing with plague event		SEOC Event Log	IL State EOC
IL	15-May-03	10:39	FBI reports that they have information that suspects dispersed aerosolized plague from backpacks - it is not known at this time if they were dispersed at additional sites or same as original attack - state police directed to get decon of possible additional releases.		Data Collector Log	IL State EOC
IL	15-May-03	10:40	IL SEOC is requesting the DMORT assist the medical examiners office of Cook County.		SEOC Event Log	IL State EOC
IL	15-May-03	10:59	IL SEOC reports all SNS distribution sites verified open and operational		SEOC Event Log	IL State EOC
IA	15-May-03	11:06	The Governor of Wisconsin sent a request to FEMA Region V which was passed to DHS EP&R for a disaster declaration: The Governor's request dated May 15, 2003 satisfies the various statutory and regulatory requirements of Public Law 93-288, as amended. The Governor has requested a major disaster declaration for the counties of Kenosha, Milwaukee, and Racine. As a result of an outbreak of Pneumonic Plague, the Governor implemented the State Emergency Plan on May 15, 2003 and declared a state emergency for these counties on May 15, 2003.		Data Collector Log	DOT CMC
IL	15-May-03	12:30	Report from Chicago EOC that plague is still present at Union station, United Center, O'Hare		Data Collector Log	Chicago JOC
IL	15-May-03	14:00	From IDPH to Dept. of State Liaison: VNN report stated IDPH did not want assistance from other nations due to lesser quality of health care & language barrier. IDPH viewed this as arrogance and requested to know who made this statement		Agency Log	DOS Liaison at IDPH
IL	15-May-03	14:20	FBI announces United Center, Union Station, and Terminal 3 at O'Hare cleared as crime scenes. US EPA says they can be opened to the public.		SEOC Event Log	IL State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	15-May-03	16:10	IL SEOC received request from FBI HMRU unit. Request asks for 2 HazMat officers from 5th CST to assist in operations. CST soldiers are available. Adjutant General has been notified and approved the mission request, with one stipulation - if CST gets talked by State/Feds as a team, 2 soldiers will return to CST control for mission support.		SEOC Event Log	IL State EOC
IL	15-May-03	16:15	IL SEOC received EmNet Emergency Message from IL JOC: FEMA Region V ROC has indicated that the National Homeland Security Advisory System level will be lowered from Red to Orange with the EXCEPTION of Chicago and New York City, which shall remain at Red.		SEOC Event Log	IL State EOC
IL	15-May-03	16:15	Chicago Department of Health & Human Services notifies Chicago OEM of reduced alert status from "Red" to "Orange" nationwide except Chicago and New York City.		Data Collector Log	Chicago EOC
IL	15-May-03	16:50	Chicago EOC receives formal notification that Nationwide Threat level lowered from Red to Orange except for New York City and Chicago		Data Collector Log	Chicago EOC
IL	15-May-03	20:38	JOC received Update from Chicago Fire Department regarding crash at Midway Airport: helicopter was completely destroyed, 10 dead, 51 serious injuries, 59 minor and 79 minimal. CPD says that crash was an accident and not terrorist attack (corresponds to MSEL # 3083).		Data Collector Log	JOC (IL)
IL	15-May-03	20:40	As of 19:30, biological testing results are as follows per the Chicago HMRT and EPA: O'Hare - neg. for <i>Yersinia Pestis</i> ; Union Station - neg. for <i>Yersinia Pestis</i> ; United Center - Positive for <i>Yersinia Pestis</i> .		Data Collector Log	JOC (IL)

	Integrated Acronym List
ABS	Arson Bomb Squad
AMS	Aerial Measuring System
ARAC	Atmospheric Release Advisory Capability
ASPA	Assistant Secretary, Public Affairs
ATF	[Bureau of] Alcohol, Tobacco, and Firearms
BC	British Columbia [CAN]
BDC	Bomb Data Center
BICE	Bureau of Immigration and Customs Enforcement
BOLO	Be On Look Out
BOMA	Building Owner and Managers Association
Ca DTPA	[trisodium] Calcium Diethylenetriamine Pentaacetic Acid
CAT	Crisis Action Team
CBP	Customs and Border Patrol
CCC	Crisis Coordination Center
CCDPH	Cook County Department of Public Health
CCSEMA	Cook County Sheriff's Emergency Management Agency
CDC	Centers for Disease Control [and Prevention]
CDRG	Catastrophic Disaster Response Group
Ce	Cesium
CEPPO	Chemical Emergency Preparedness and Prevention Office
CFD	Chicago Fire Department
CMC	Crisis Management Center
CMRT	Consequence Management Response Team
COOP	Continuity of Operations Plans
CPD	Chicago Police Department
CST	Civil Support Team
CTA	Chicago Transit Authority
DC	District of Columbia
DEST	Domestic Emergency Support Team
DHS	Department of Homeland Security
DMAT	Disaster Medical Assistance Team
DMAT	Disaster Medical Assistance Team
DMORT	Disaster MORTuary Team
DOH	Department of Health
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DPH	Department of Public Health
DPMU	Disaster Portable Morgue Unit
DTPA	Diethylenetriamine Pentaacetic Acid
EDP	Emergency Disaster Plan
EIS	Epidemic Intelligence Service
EMD	Emergency Management Division
EMNET	Emergency Network
EMSHG	Emergency Management Strategic Health Care Group
EOC	Emergency Operations Center
EPA	Environmental Protection Agency

ERT	Evidence Response Team
ESF	Emergency Support Function
ESF-10	ESF Hazardous Materiel
ESF-8	Emergency Support Function 8 (Health and Medical Services)
ESF-9	Emergency Support Function 9 (Urban Search and Rescue)
EST	Emergency Support Team
EST	Emergency Support Team
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FPS	Federal Protective Service
FRA	Federal Railroad Administration
FRMAC	Federal Radiological Management Center
FTA	Federal Transit Administration
GLODO	Group for the Liberation of Orangeland and the Destruction of Others
Gm	Gram
GSA	General Services Administration
HAN	Health Alert Network
HAZMAT	Hazardous Materials
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HMRT	Hazardous Materials Response Team
HMRU	Hazardous Materials Response Unit
HMRU	Hazardous Materials Response Unit
HMRU	Hazardous Materials Response Unit
HQ	Headquarters
HRT	Hostage Rescue Team
HSAS	Homeland Security Advisory System
HSAS	Homeland Security Alert Status
HVAC	High Volume Air Conditioning
IC	Incident Command(er)
ICE	Immigration and Customs Enforcement
ICP	Incident Command Post
ICS	Incident Command System
IDPH	Illinois Department of Public Health
IEMA	Illinois Emergency Management Agency
IL SEOC	Illinois State Emergency Operations Center
IMERT	Illinois Medical Emergency Team
IMSURT	International Medical SURgical Response Team
IOF	Interim Operating Facility
IOHNO	Illinois Operational Headquarters and Notification Office
ISP	Illinois State Police
JIC	Joint Information Center
JOC	Joint Operations Center
JTF	Joint Task Force

LQRAM	Large Quantity RadioActive Material
MARSEC	Maritime Security
MCC	Master Control Cell
MCI	Mass Casualty Incident
MERRT	Medical Emergency Radiological Response Team (Veterans Affairs)
METRA	Metropolitan Rail Agency
MRV	Mobile Response Vehicle
MSEL	Master Scenario Event List
MST	Management Support Team
NAWAS	NAtional WArning System
NCEH	National Center for Environmental Hazards
NCID	National Center for Infectious Diseases
NDMS	National Disaster Medical System
NJTTF	National Joint Terrorism Task Force
NMRT	National Medical Response Team
NMRT	National Medical Response Team
NNSA	National Nuclear Security Administration
NPP	Nuclear Power Plant
NPS	National Pharmaceutical Stockpile
NRC	Nuclear Regulatory Commission
NRT	National Response Team
OEM	Office of Emergency Management
OEMC	Office of Emergency Management Communications
ONCRC	Office of National Capitol Region Coordination
OSC	On-Scene Coordinator
OSHA	Occupational Safety and Health Administration
OSLGC	Office of State and Local Government Coordination (DHS)
PAT	Preliminary Assessment Team
PCR	Polymerase Chain Reaction
PFO	Principle Federal Official
PHSKC	Public Health-Seattle & King County
PIO	Public Information Officer
PPE	Personal Protective Equipment
Pu	Plutonium
RAP	Radiological Assistance Program
RAP[T]	Radiological Assistance Program [Team]
RDD	Radioloigical Dispersion Device
RDD	Radiological Dispersal Device
REAC	Radiological Emergency Assistance Center
REOC	Regional Emergency Operations Center
RHA	Regional Health Administrator
ROC	Regional Operations Center
RSAN	Roam Secure Alert Network
RTA	Regional Transportation Authority
S-60	DOT Office of Intelligence and Security
SABT	Special Agent Bomb Technician
SAC	Special Agent in Charge
SCC	Secretary's Command Center

SEATAC	Seattle-Tacoma [Airport]
SEOC	State Emergency Operations Center
SERT	[HHS] Secretary's Emergency Response Team
SFD	Seattle Fire Department
SHL	State Health Liaison
SIOC	Strategic Information Operations Center
SME	Subject Matter Experts
SNS	Strategic National Stockpile
SODO	South Of DOWntown [Seattle]
SPD	Seattle Police Department
SPU	Seattle Public Utilities
STB	Surface Transportation Board
SWAT	Special Weapons And Tactics
SWMDT	State Weapons of Mass Destruction Team
TFR	Temporary Flight Restriction
TOPS	TOPOFF Pulmonary Syndrome
TRT	Tactical Response Team
TSA	Transportation Security Administration
UC	Unified Command
UCS	Unified Command System
US&R	Urban Search and Rescue
USAR	Urban Search and Rescue
USMS	United States Marshal Service
USSS	United States Secret Service
VACO	Veterans Affairs Central Office
VCC	Venue Control Cell
VMI	Vendor Managed Inventory
VNN	Virtual News Network
WA	Washington [State]
WH	White House
WMD	Weapons of Mass Destruction
Zn DTPA	[trisodium] Zinc Diethylenetriamine Pentaacetic Acid

	Washington Acronyms
ABS	Arson Bomb Squad
DEST	Domestic Emergency Support Team
DMAT	Disaster Medical Assistance Team
DOH	Department of Health
EMD	Emergency Management Division
EOC	Emergency Operations Center
ERT	Evidence Response Team
ESF	Emergency Support Function
EST	Emergency Support Team
FEMA	Federal Emergency Management Agency
HAZMAT	Hazardous Materials
HMRT	Hazardous Materials Response Team
HMRU	Hazardous Materials Response Unit
IC	Incident Command(er)
ICS	Incident Command System
IOF	Interim Operating Facility
JOC	Joint Operations Center
MARSEC	Marine Security
MCI	Mass Casualty Incident
MSEL	Master Scenario Event List
NJTTF	National Joint Terrorism Task Force
NMRT	National Medical Response Team
PHSKC	Public Health-Seattle & King County
PIO	Public Information Officer
RAP	Radiological Assistance Program
RDD	Radiological Dispersion Device
ROC	Regional Operations Center
SABT	Special Agent Bomb Technician
SEOC	State Emergency Operations Center
SEOC	Seattle Emergency Operations Center
SFD	Seattle Fire Department
SHL	State Health Liaison
SIOC	Strategic Information Operations Center
SODO	South of Downtown
SPD	Seattle Police Department
SPU	Seattle Public Utilities
TFR	Temporary Flight Restriction
TSA	Transportation Security Administration
UC	Unified Command
UCS	Unified Command System
USAR	Urban Search and Rescue
VCC	Venue Control Cell
VNN	Virtual News Network

	Interagency Acronyms
ASPA	Assistant Secretary, Public Affairs
AMS	Aerial Measuring System
ARAC	Atmospheric Release Advisory Capability
ATF	[Bureau of] Alcohol, Tobacco, and Firearms
BC	British Columbia [CAN]
BDC	Bomb Data Center
BICE	Bureau of Immigration and Customs Enforcement
BOLO	Be On Look Out
Ca DTPA	[trisodium] Calcium Diethylenetriamine Pentaacetic Acid
CAT	Crisis Action Team
CBP	Customs and Border Patrol
CCC	Crisis Coordination Center
CDC	Centers for Disease Control [and Prevention]
CDRG	Catastrophic Disaster Response Group
Ce	Cesium
CEPPO	Chemical Emergency Preparedness and Prevention Office
CMC	Crisis Management Center
CMRT	Consequence Management Response Team
COOP	Continuity of Operations Plans
DC	District of Columbia
DEST	Domestic Emergency Support Team
DHS	Department of Homeland Security
DMAT	Disaster Medical Assistance Team
DMORT	Disaster MORTuary Team
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DPMU	Disaster Portable Morgue Unit
DTPA	Diethylenetriamine Pentaacetic Acid
EMSHG	Emergency Management Strategic Health Care Group
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
ERT	Emergency Response Team
ERT	Evidence Response Team
ESF	Emergency Support Function
ESF-10	ESF Hazardous Materiel
ESF-8	Emergency Support Function 8 (Health and Medical Services)
ESF-9	Emergency Support Function 9 (Urban Search and Rescue)
EST	Emergency Support Team
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FPS	Federal Protective Service
FRA	Federal Railroad Administration
FRMAC	Federal Radiological Management Center

FTA	Federal Transit Administration
GLODO	Group for the Liberation of Orangeland and the Destruction of Others
GSA	General Services Administration
HAN	Health Alert Network
HHS	Health and Human Services
HMRU	Hazardous Materials Response Unit
HQ	Headquarters
HRT	Hostage Rescue Team
HSAS	Homeland Security Advisory System
ICE	Immigration and Customs Enforcement
IMSURT	International Medical SURgical Response Team
JIC	Joint Information Center
JOC	Joint Operations Center
JTF	Joint Task Force
LQRAM	Large Quantity RadioActive Material
MARSEC	Maritime Security
MCC	Master Control Cell
MCCUE	Master Control Cell Un-Evaluator
MERRT	Medical Emergency Radiological Response Team (Veterans Affairs)
MRV	Mobile Response Vehicle
MST	Management Support Team
NAWAS	NAtional Warning System
NCEH	National Center for Environmental Hazards
NCID	National Center for Infectious Diseases
NCID	National Center for Infectious Diseases
NDMS	National Disaster Medical System
NMRT	National Medical Response Team
NNSA	National Nuclear Security Administration
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NRT	National Response Team
ONCRC	Office of National Capitol Region Coordination
OSC	On-Scene Coordinator
OSHA	Occupational Safety and Health Administration
OSLGC	Office of State and Local Government Coordination (DHS)
PAT	Preliminary Assessment Team
PFO	Principle Federal Official
PPE	Personal Protective Equipment
Pu	Plutonium
RAP[T]	Radiological Assistance Program [Team]
RDD	Radiological Dispersal Device
REAC	Radiological Emergency Assistance Center
REOC	Regional Emergency Operations Center
RHA	Regional Health Administrator
ROC	Regional Operations Center
RSAN	Roam Secure Alert Network
S-60	DOT Office of Intelligence and Security
SAC	Special Agent in Charge
SCC	Secretary's Command Center

SEATAC	Seattle-Tacoma [Airport]
SERT	[HHS] Secretary's Emergency Response Team
SIOC	Strategic Information Operations Center
SME	Subject Matter Experts
SNS	Strategic National Stockpile
SODO	South Of DOWntown [Seattle]
STB	Surface Transportation Board
SWAT	Special Weapons And Tactics
TFR	Temporary Flight Restriction
TSA	Transportation Security Administration
US&R	Urban Search and Rescue
USMS	United States Marshal Service
USSS	United States Secret Service
VACO	Veterans Affairs Central Office
VCC	Venue Control Cell
VNN	Virtual News Network
WA	Washington [State]
WH	White House
WMD	Weapons of Mass Destruction
Zn DTPA	[trisodium] Zinc Diethylenetriamine Pentaacetic Acid

	Illinois Acronyms
BOMA	Building Owner and Managers Association
CCDPH	Cook County Department of Public Health
CCSEMA	Cook County Sheriff's Emergency Management Agency
CFD	Chicago Fire Department
CPD	Chicago Police Department
CST	Civil Support Team
CTA	Chicago Transit Authority
DHS	Department of Homeland Security
DMAT	Disaster Medical Assistance Team
DPH	Department of Public Health
EDP	Emergency Disaster Plan
EIS	Epidemic Intelligence Service
EMNET	Emergency Network
EPA	Environmental Protection Agency
GLODO	Group for the Liberation of Orangelandia and the Destruction of Others
Gm	Gram
HAN	Health Alert Network
HazMat	Hazardous Materials
HIPAA	Health Insurance Portability and Accountability Act
HMRT	Hazardous Materials Response Team
HMRU	Hazardous Materials Response Unit
HSAS	Homeland Security Alert Status
HVAC	High Volume Air Conditioning
ICP	Incident Command Post
IDPH	Illinois Department of Public Health
IEMA	Illinois Emergency Management Agency
IL SEOC	Illinois State Emergency Operations Center
IMERT	Illinois Medical Emergency Team
IOHNO	Illinois Operational Headquarters and Notification Office
ISP	Illinois State Police
JOC	Joint Operations Center
METRA	Metropolitan Rail Agency
NDMS	National Disaster Medical System
NPS	National Pharmaceutical Stockpile
OEM	Office of Emergency Management
OEM	Office of Emergency Management
OEMC	Office of Emergency Management Communications
PCR	Polymerase Chain Reaction
PIO	Public Information Officer
PPE	Personal Protective Equipment
RTA	Regional Transportation Authority
SNS	Strategic National Stockpile
SWMDT	State Weapons of Mass Destruction Team
TOPS	TOPOFF Pulmonary Syndrome
TRT	Tactical Response Team
VMI	Vendor Managed Inventory
VNN	Virtual News Network

TOP OFFICIALS (TOPOFF) EXERCISE SERIES:

TOPOFF 2 (T2) After Action Report ANNEX B



September 30, 2003

Information contained in this document is intended for the exclusive use of T2 Exercise Series participants. Material may not be reproduced, copied, or furnished to non-exercise personnel without written approval from the Exercise Directors.

This page intentionally left

TOP OFFICIALS (TOPOFF) EXERCISE SERIES:

TOPOFF 2 (T2) After Action Report ANNEX C



September 30, 2003

Information contained in this document is intended for the exclusive use of T2 Exercise Series participants. Material may not be reproduced, copied, or furnished to non-exercise personnel without written approval from the Exercise Directors.

This page intentionally left



WASHINGTON, DC | MARYLAND | VIRGINIA



DRAFT

NATIONAL CAPITAL REGION FUNCTIONAL EXERCISE

AFTER-ACTION REPORT
MAY 12, 2003



This project was supported by the U.S. Department of Homeland Security (USDHS) Office for Domestic Preparedness (ODP). Points of view presented in this document are those of the authors and do not necessarily represent the official position of ODP.

T2 AAR #041

TABLE OF CONTENTS

Introduction.....	1
Executive Summary.....	3
Exercise Design.....	5
Purpose.....	5
Scope.....	5
Focus.....	5
Structure.....	5
Materials.....	6
Guidelines.....	6
Exercise Assumptions and Artificialities.....	6
Scenario.....	7
Exercise Objectives.....	8
Significant Findings.....	11
Coordination and Communication within Jurisdictions.....	11
Technical Issues.....	11
Change in HSAS Threat Level.....	12
Issues and Recommendations.....	13
VDEM EOC.....	13
FEMA HQ.....	15
DCEMA EOC.....	19
FBI WFO.....	22
MEMA EOC.....	24
USDHS NCR.....	27
Appendix A – Exercise Participants.....	28

INTRODUCTION

BACKGROUND – THE FACE OF TERRORISM

September 11, 2001, stands as a day that forever changed the way Americans view terrorism. The magnitude of the events shattered many long-held beliefs regarding the types of terrorist attacks the Nation might face, and has effectively shattered the image of “Fortress America” for many citizens. As former Senator Sam Nunn wrote shortly after the tragedy, “The terrorists who carried out the attack of September 11 showed there is no limit to the number of innocent lives they are willing to take. Their capacity for killing was restricted only by the power of their weapons.”

As the Nation worked to recover from the attacks on the World Trade Center, on the Pentagon, and in western Pennsylvania, this statement proved to be prophetic, as cases of anthrax exposure began to appear around the country. Cases first appeared in Florida, then New York and Washington, DC, and then in various locations across the country. Although no one has claimed responsibility for the release of anthrax, the country remains on an overall higher state of alert. Security at buildings, airports, and other facilities has increased, and government officials warn of the danger of further attacks on the Nation.

Many speak of a “new framework for national security” in which the fight against terrorism will take prominence. As President Bush stated on the first weekend after the attacks, “We haven’t seen this kind of barbarism in a long period of time. No one could have conceivably imagined suicide bombers burrowing into our society and then emerging all in the same day to fly ... U.S. aircraft into buildings full of innocent people...and show no remorse. This is a new kind ... of evil. And we understand. And the American people are beginning to understand. This crusade, this war on terrorism is going to take a while. And the American people must be patient.” As the war on terrorism continues to take shape, the world remains anxious that the next outbreak of violence could come from any direction, at any time.

As the country responds to and recovers from these attacks, citizens turn to political leaders with one question: “What will be next?” As the latest operations in the war against terrorism begin, the Nation’s leaders have reiterated the need for preparedness against all kinds of threats. Long-held taboos have been broken, and today’s terrorist has the potential to be far more deadly than ever before. The tools of the terrorist have evolved from pipe bombs and guns to massive ammonium nitrate bombs, the use of airliners as flying bombs, and the dissemination of anthrax.

Extremist and absolutist ideologies allow perpetrators to take extraordinary measures in support of their goals. At the forefront of this in the international arena is al Qaeda, a group of Islamic militants led by Osama bin Laden. Having claimed credit for the September 11 attacks, bin Laden declared that more will occur. In recent years, he has stated that acquiring weapons of mass destruction (WMD) was a goal of his group. As President Bush said in November 2001, "These terrorist groups seek to destabilize entire nations and regions. They are seeking

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

chemical, biological, and nuclear weapons. Given the means, our enemies would be a threat to every nation and, eventually, to civilization itself.”

Because of this, the use of WMD by terrorists has received even greater prominence in the United States as a major national security concern. As Senator Nunn wrote, “We have had a look at the face of terrorist warfare in the 21st century, and it gives us little hope that if these groups gained control of nuclear, biological, and chemical weapons they would hesitate to use them.”

In March 2002, the Office of Homeland Security (OHS) developed a national alert system that responds to concerns about terrorist attacks. This system disseminates information regarding the risk of terrorist attacks to all levels of government and the American people. There are five color-coded threat levels associated with the level of risk of terrorist attacks and what protective measures should be taken.



When confronted with the question of “What will be next?” leaders cannot say for sure. However, they reiterate that we as a Nation will be committed for the long term, that we must steel our resolve, and that we must endeavor to ensure that our communities are as prepared as possible to respond to any future attacks.

With that resolve in mind, The Homeland Security Act of 2002 was signed into law thus changing the OHS and creating the U.S. Department of Homeland Security (USDHS) which became operational on March 1, 2003.

EXECUTIVE SUMMARY

The National Capital Region Functional Exercise (NCRFE) was conducted on May 12, 2003, in the National Capital Region (NCR). This included the Federal Emergency Management Agency Headquarters (FEMA HQ) in Washington, DC; The District of Columbia Emergency Management Agency Emergency Operations Center (DC EMA EOC) in Washington, DC; the Federal Bureau of Investigation Washington Field Office (FBI WFO) in Washington, DC; the Virginia Department of Emergency Management Emergency Operations Center (VDEM EOC) in Richmond, VA; and the Maryland Emergency Management Agency Emergency Operations Center (MEMA EOC) in Reisterstown, MD, and the U.S. Department of Homeland Security (USDHS), Office of the National Capital Region Coordinator (ONCRC) in Washington, DC. The exercise was conducted under the aegis of the USDHS, Office for Domestic Preparedness (ODP), in cooperation with the NCR. The NCRFE was designed to coincide with the TOPOFF2 (T2) full-scale exercise in order to assist the NCR jurisdictions in assessing their preparedness and coordination in response to a general attack on the Nation and changes to the Homeland Security Advisory System threat level. The T2 scenario involved a radiological dispersal device (RDD) explosion in Seattle, WA. The NCRFE was a no-fault, functional communications response to the weapons of mass destruction (WMD) terrorism event in Seattle, WA, as well as a simulated but credible threat to the National Capital Region. The NCRFE was designed by the Community Research Associates (CRA) USDHS Exercise Support Team.

The NCRFE scenario incorporated two events: a credible threat of a terrorist event directed at five U.S. cities and a radiological dispersal device (RDD) explosion in Seattle, WA. The exercise included two modules. In Module One (which was simulated as six days earlier, May 6, 2003), the Homeland Security Advisory System (HSAS) national threat level was raised from Yellow to Orange. In Module Two, an RDD exploded in Seattle, with a subsequent change in threat level from Orange to Red. This functional exercise scenario allowed the jurisdictions to assess their overall communication and coordination within the National Capital Region.

One of the exercise's main objectives was to assess the relationship among all jurisdictions within the National Capital Region. Information-sharing and coordination proved to be extremely important in mitigating a terrorist event in the NCR. The DC EOC seemed to be controlling most of the flow of information to Maryland and Virginia. MEMA EOC representatives felt that other than a conference call, they were pulling information from the other jurisdictions, rather than having the information being pushed to them. Also, it was noted that it would have been beneficial to have representatives from FEMA, VA, and MD in the DC EOC during the exercise to further enhance the jurisdictions' relationships.



National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

Technical communications issues within each EOC proved to be an exercise obstacle but all jurisdictions were able to properly communicate with each other. FEMA HQ had issues with videoconferencing, although they noted that in a real-world setting, they would have had the Information Technology (IT) support they needed. The DC EOC had some technical problems with their internal E-Team software that supported their EOC tracking system. At VDEM EOC, sufficient security clearances were not available for the use of the secure video teleconferencing (VTC) system. Changes in homeland security require that a National Guard representative be present at all times that secure VTC equipment is being used.



Overall, the exercise was very successful. DC EOC felt that they had good control of the situation, and that they were disseminating information efficiently. MEMA EOC felt that all of their objectives were met, but that exercise information should have been disseminated more often (from the DC EOC). VDEM EOC needs more funding in order to participate more effectively in exercises. FEMA was very effective throughout the exercise in their role as the coordinator of Federal assets. USDHS's new role of providing policy guidance and coordination for the NCR was accomplished without any problems. The only major question that was not addressed during this exercise was how well the communications network connection would work between the Federal agencies' emergency relocation sites.

EXERCISE DESIGN

PURPOSE

The National Capital Region Functional Exercise (NCRFE) was designed to coincide with the TOPOFF 2 (T2) full-scale exercise (FSE) in order to assist National Capital Region (NCR) jurisdictions in assessing their preparedness and coordination in response to a general attack on the Nation and changes to the Homeland Security Advisory System (HSAS) threat level.

SCOPE

The NCRFE was conducted on May 12, 2003, at various locations within the NCR, including the District of Columbia Emergency Operations Center (DC EOC), the State of Maryland EOC, the Commonwealth of Virginia EOC, the Federal Bureau of Investigation (FBI) Washington Field Office (WFO), the Federal Emergency Management Agency Headquarters (FEMA HQ) at 500 C. Street, and the Office of the National Capital Region Coordinator, U.S. Department of Homeland Security (ONCRC, USDHS). Approximately 100 individuals participated in the exercise.

Focus

The NCRFE events focused on the following activities:

- Observe or exercise NCR coordination functions.
- Observe use of physical communications facilities.
- Reinforce established policies and procedures.
- Measure resource adequacy.
- Assess inter-jurisdictional relations.

The NCRFE was played in real time. However, some responses and actions required additional time or accelerated time in order to meet exercise objectives.

STRUCTURE

The NCRFE examined the connectivity, in a free-play environment, of various NCR agencies as they related to the exercise scenario. The NCR agencies that were represented are:

- Virginia Department of Emergency Management
- Federal Emergency Management Agency
- District of Columbia Emergency Management Agency
- Federal Bureau of Investigation—Washington Field Office
- Maryland Emergency Management Agency
- Office of the National Capital Region Coordinator, U. S. Department of Homeland Security

National Capital Region Functional Exercise

The NCRFE was designed to exercise individual capabilities, multiple functions, activities within a function, or interdependent groups of functions. It was generally focused on exercising the plans, policies, procedures, and staffs of the managerial or direction and control nodes of each jurisdiction's emergency management agency. Generally, the use of response resources was simulated, and events were projected through an exercise scenario and event updates to stress or drive activity at the management level.

Each controller/evaluator involved in the execution of the exercise received a briefing prior to the exercise that described their duties and responsibilities in depth. They were provided with a C/E Handbook with detailed instructions about the exercise and the scenario, as well as their roles and responsibilities. Evaluation forms for each controller and evaluator were also provided. An EXPLAN was distributed that contained general information regarding basic issues, such as the purpose of the exercise and rules of conduct.

- The exercise was not a test, but rather a no-fault learning experience.
- The exercise was intended to be in an open, low-stress environment.
- This exercise served as a realistic setting within which participants were given the opportunity to implement previously identified adjustments in standard operating policies and procedures.
- Responses were based on current capabilities (i.e., only existing abilities and assets).

The following general assumptions applied to the NCRFE:

- The goals and objectives of the exercise were consistent with functional area operations, technical plans, and procedures, whenever possible.
- NCR agencies, along with the USDHS Office for Domestic Preparedness (ODP) and/or its contractor (Community Research Associates [CRA]), were major participants and/or had significant roles in coordinating the exercise.

Artificialities and Constraints

Although there were a number of artificialities and constraints that may have detracted from exercise realism, the NCRFE planners and participants recognized and accepted that some artificialities and simulations were necessary to carry out the exercise.

SCENARIO

Several variables were selected by the NCRFE planners and used in the development of the scenario and overall structuring of the exercise:

- The NCRFE was connected with the T2 FSE, but was played separately.
- Background intelligence events in Module One triggered a change in the HSAS national threat level from Yellow to Orange.
- A WMD event involving an RDD in Seattle, WA, in Module Two triggered a change in the HSAS national threat level from Orange to Red.

Module One. Module One was played as if it were May 6, 2003, and used the T2 background information that built up a credible terrorism threat against five major U.S. cities, triggering an HSAS threat level change from Yellow to Orange.

Module Two. Module Two was played in real time on May 12, 2003, and focused on an RDD attack in Seattle, WA, and the subsequent HSAS threat level change from Orange to Red.

EXERCISE OBJECTIVES

NCRFE was designed to assist Federal, State, and local agencies located in the NCR in coordinating a response to changes in the national threat level, as a potential but credible region-wide threat of WMD terrorism evolves. Seven specific objectives for the exercise are listed below with comments:

1. **Objective:** Identify and exercise communication capabilities (voice, fax, data, and video) among NCR jurisdictions.

Discussion: This major objective was clearly met during the planning and execution phase of the exercise. Voice, fax, and data connectivity worked fine among all of the players. However, technical communication issues within each EOC proved to be an obstacle. A video connection among all NCR jurisdictions is needed; not all jurisdictions had the proper equipment to have a video conference meeting.

Recommendation: Each NCR jurisdiction needs to have its communications divisions review the requirements for full video conferences and establish the budget to gain the equipment and capability.

- 2. Objective: Review information-sharing capabilities among NCR jurisdictions.**

Discussion: This objective was met by each player jurisdiction. During the course of the short exercise, information was passed among the organizations via voice, fax, and computer systems. Had the exercise lasted longer, the information-sharing capabilities would have continued to improve.

Recommendation: The NCR jurisdictions should continue to exercise their communications capabilities among the organizations on a day-to-day basis to ensure that each system works and that there is a continuing flow of information that is second nature to all involved in this process. This objective should be first and foremost in all future NCR exercises.

3. **Objective:** Develop and coordinate consistent public information strategies.

Discussion: This objective was addressed very carefully by each jurisdiction's public affairs officer (PAO) before and during the exercise. Each PAO connected with his or her counterpart, and opened all channels of communication to ensure that the public information strategies were properly coordinated. Again, in a longer exercise, this function would have been exercised in depth.

Recommendation: The PAOs of each NCR jurisdiction should maintain contact with each other on a regular basis in order to keep the lines of communication open year-round.

National Capital Region Functional Exercise
DRAFT After-Action Report DRAFT

4. **Objective:** Review connectivity within and among NCR agencies in accordance with USDHS procedures.

Discussion: Early in the exercise, all of the player NCR agencies made voice, fax, and data connections with their counterparts at all levels (policymakers and staff). Several telephone conference calls were made among the NCR agencies, but the use of radios and video conferencing was not tested. It should be noted that because of the short length of time for this exercise (and the scope of the scenario), the FEMA Interim Operating Facility (IOF) and the USDHS operations center were not used or tested in this exercise.

Recommendation: The NCR should schedule a longer and more extensive NCR WMD response exercise in the near future, which will force the testing of all NCR emergency operations facilities (and communications) at the Federal, State, and local levels within the NCR.

5. **Objective:** Coordinate the decision-making processes of all three jurisdictions with FEMA and the FBI.

Discussion: The decision-making processes of all three major NCR jurisdictions were completely coordinated with FEMA, the FBI, and USDHS. Each agency was connected to several senior-level conference calls, which ensured that the decision-making process was properly coordinated.

Recommendation: The major NCR jurisdictions should ensure that the senior policy council members continue to meet on a regular basis, and hold at least one general teleconference each month to discuss a major policy issue.

6. **Objective:** Review 7 of the NCR's "8 Commitments to Action":

Terrorism Prevention
Citizen Involvement in Preparedness
Decision Making and Coordination
Emergency Protective Measures
Infrastructure Protection
Media Relations and Communication
Mutual Aid

Discussion: All of the Commitments to Action listed above received at least a review of required actions by each major jurisdiction during this exercise. The stated goal of the exercise was to follow the elevated threat level recommendations of USDHS (based on the T2 threat scenario), and review the coordinated actions that need to be taken in the NCR for these areas of concern. Each jurisdiction understood many of the required actions, but because of the short length of the exercise, it was impossible to completely test each of these rather complex subjects.

Recommendation: The NCR should take at least three months to plan a longer and more specific exercise that will allow a thorough testing of each of these important aspects of a coordinated response to a terrorist WMD attack on the region. This type of exercise should run about 8 to 12 hours in length.

7. **Objective:** Improve the NCR's readiness to respond to any possible act of terrorism.

Discussion: Every practice exercise that can be conducted before a real event occurs improves the readiness of an organization, agency, government, or region to respond to a real incident. This exercise was the first step in that readiness improvement process for the NCR region. Most State-level governments and military organizations believe that daily and weekly individual/small organizational training, followed by quarterly or biannual large organization training or exercising, is the proper way to prepare an organization or agency for the real event. The NCR jurisdictions should do no less.

Recommendation: The NCR Senior Policy Council staff should prepare a three-year, region-wide exercise plan and schedule that can be funded and followed to improve the NCR jurisdictions' preparations for a terrorist WMD attack on the region. Most experts in this field truly believe that it is not a matter of "if" but "when" an attack will occur on the very high-profile District of Columbia and consequently the NCR.

SIGNIFICANT FINDINGS

COORDINATION AND COMMUNICATION AMONG JURISDICTIONS

Before the NCRFE took place, a major concern was the communication and coordination among all NCR jurisdictions (MD, VA, DC, FEMA, USDHS-NCR) in a terrorist event. Although the NCR was not an imminent target for a terrorist event in the exercise, it was understood that being in or near the Nation's capital, as well as having a credible threat to five U.S. cities, required proper action (i.e., communication and coordination among all jurisdictions) in order to protect its citizens. Since the NCR comprises several jurisdictions, it was imperative to assess and enhance their communication and coordination effectiveness during a terrorist event.

- It seemed that the District of Columbia Emergency Management Agency (DC EMA) was controlling most of the flow of information to the other States (MD and VA).
- The Maryland Emergency Management Agency (MEMA) had the most difficulty with communication and information sharing during the exercise. Conference calls were established that included FEMA, USDHS, MD, VA, and DC. It seemed that there was little independent information sharing that took place outside of the conference call format. At no time outside of the prearranged conference calls was DC or VA queried as to how they were handling these issues of concern.
- Representatives from FEMA, VA, and MD were not present in the DC EOC during the exercise. It was stated, however, that in a real-world setting, representatives would be present.

TECHNICAL ISSUES

There were a number of technical issues in each EOC that appeared to hinder the ability of the exercise participants to play efficiently.

- At FEMA HQ, video conferencing was inaccessible during the exercise due to technical problems.
- At DC EOC, computer printers were overloaded; exercise participants were kept waiting for their printed material. The location of the printers also obstructed the view of the Operations Chief. The location of the printers also made it difficult for the participants to move freely throughout the DC EOC to gather information.
- The DC EOC also had difficulties with the new E-Team Software, although Information Technology (IT) representatives were present to help with any problems that participants encountered (such as with training).

- At VDEM EOC, sufficient security clearances were not available for the use of the video teleconferencing system. Changes in Homeland Security policy required that a National Guard representative be present at the VDEM EOC each time that secure VTC equipment is being used.

It is understood that technical issues are ubiquitous and difficult to avoid, and during a real-world situation, things would have gone differently. However, it should be stated that IT support should be available and proper clearances ensured, in order to enhance communication among jurisdictions. Coordination and communication were exercised well, and all participating agencies understood that they could be improved.

CHANGE IN HSAS THREAT LEVEL

The HSAS threat level change is a recommendation for each State. Following the HSAS threat level change from Orange to Red after the event in Seattle, questions arose in MEMA and VDEM regarding whether it was necessary to change the threat level throughout their entire State(s).

- Following the terrorist event in Seattle and subsequent change in threat level from Orange to Red, FEMA immediately responded by activating and dispatching the NCR ERT-N to an emergency relocation site in Maryland, and was kept apprised of all actions thereafter.
- VA controllers noted that VDEM EOC staff verbally questioned whether the entire State should be elevated to threat level Red.
- MD controllers had a lengthy discussion regarding whether the entire State of Maryland should elevate the threat level to Red, or just raise the level within selected vulnerable jurisdictions. MD controllers also noted that the MD decisionmakers recognized distinct liability issues associated with this decision.

ISSUES AND RECOMMENDATIONS

**VIRGINIA DEPARTMENT OF EMERGENCY MANAGEMENT
EMERGENCY OPERATIONS CENTER
RICHMOND, VA**

General Statement

The initial information and injects were handled well by the EOC staff. Appropriate notifications to State agencies and the Governor's Office and external notifications by fax and the VDEM EOC web site were made. All State agencies were notified within ten minutes of the beginning of the exercise.



The State Police complex that houses the EOC was locked down, one point of entry was established, and mandatory ID use was instituted. The EOC paged the Commonwealth Preparedness Working Group (CPWG) for a conference call, which took place at 1:32 p.m. The CPWG conducted a well-organized conference call with State agencies, and used a checklist for those agencies that were identified to participate in the call. A status review by each agency director was given, as well as the current condition of the EOC.

As exercise play continued in the NCR, FEMA began notifying area representatives. Ms. Cindy Causey, the VDEM NCR field representative, was notified of the incident by FEMA directly on her cell phone. No additional notifications were made to the VDEM EOC. Dual notification should be done by FEMA, however, to ensure that the appropriate agency representative is notified.

During the exercise, it was requested that a video conference call be held among the VA, MD, and DC EOCs. The Virginia EOC cannot open a secure VTC until a National Guard representative is present. The VDEM EOC staff is still undergoing new security clearance investigations.

During exercise play, the VDEM EOC communications center underwent a scheduled dispatcher shift change. Shift change briefings were conducted and there were no noted problems.

All tasks and requests presented to VDEM EOC staff were handled in a timely and appropriate manner. Coordination on the State level was excellent. Policies and procedures are in place that identify tasks associated with an EOC standup, State coordination activities, and regional coordination activities.

Overall, the VDEM EOC handled the scenario extremely well.

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

Specific issues identified at the VDEM EOC:

- FEMA notification to VDEM NCR representative
- VDEM EOC secure video communications
- EOC facilities

Issue: FEMA Notification to VDEM NCR Representative

Observation: During the exercise, FEMA placed a cell phone call directly to Cindy Causey, the VDEM NCR field representative. Although this call was handled appropriately and showed the local coordination between VDEM and FEMA, if Ms. Causey had not been available or if her phone had been out of a service area, no one at VDEM would have been notified.

Recommendation: VDEM EOC should develop a policy that provides all agencies with the central communications phone number for all emergency-related issues. This will funnel all communications directly to the EOC, who can then pass that information on to the appropriate person.

Issue: VDEM EOC Secure Video Communications

Observation: VDEM EOC has the capability and equipment to use a secure video teleconferencing system. Because of changes in Homeland Security policy, existing security clearances of the staff were removed and new clearances are still being investigated. Consequently, a National Guard representative must be present at the VDEM EOC each time that secure VTC equipment is being used.

Recommendation: Security clearances should be expedited to allow the immediate use of secure VTC equipment.

Issue: EOC Facilities

Observation: As a key member of the NCR, Virginia is home to many critical Federal facilities, such as the Pentagon. In this new day of heightened security, and the need to handle complicated and specialized emergency coordination activities, the VDEM EOC is a small and outdated facility. Satellite video downlink capability was not available during the NCR functional exercise.

Recommendation: Although engineering drawings are available to demonstrate the potential of a new VDEM EOC, there is currently no funding for construction. Construction should be a priority, however, and the availability of Federal funds should be investigated.

National Capital Region Functional Exercise After-Action Report

**FEDERAL EMERGENCY MANAGEMENT AGENCY
HEADQUARTERS
WASHINGTON, DC**

General Statement

The NCRFE was designed to allow the principal jurisdictions of the NCR (DC, VA, and MD) to exercise their communications and decision-making coordination during an elevated threat of terrorism that uses WMD in or near the NCR. This process had to be tied into and coordinated with the actions of key elements of the Federal Government, or in this case, the FBI, FEMA, and USDHS.



The major issue facing the entire exercise was: Could these major jurisdictions communicate and coordinate what they were doing to protect their citizens, infrastructure, and communities with each other and the Federal Government in an effective manner? Traditionally, FEMA, the FBI, and the governments of the three major jurisdictions (VA, MD, and DC) have learned to communicate and coordinate through their emergency management agencies during times of crisis response to disaster-related problems. This has resulted in a foundation upon which the current process is being built. USDHS is the only new player in this process, and is quickly integrating its organization into the control of the response system. The NCRFE showed that this system will work and that the major objectives were met (as well as possible in a four- to five-hour functional or command post exercise).

The individuals representing FEMA during NCRFE did a superb job. The Federal Coordinating Officer (FCO) (Mr. Davies) was acutely aware of FEMA's roles and responsibilities and was not afraid to make recommendations and decisions when called for by the exercise scenario. He and his team analyzed the information as it was received, decided on what course of action was indicated and prudent, and then either implemented it or recommended to his superiors that it be implemented. The communication and coordination among FEMA, USDHS, and the NCR EOCs was outstanding.

Specific issues identified at FEMA:

- Location of NCR crisis management staffs
- Relationship between USDHS and FEMA during this type of crisis management
- Change in threat level from yellow to orange
- Coordination and information sharing within the NCR
- Press inquiries to FEMA
- Fax directing that all States be informed of the threat level change and specific actions
- Post-Seattle blast actions

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

- Virtual News Network (VNN) broadcasts
- Actions taken after RDD was confirmed in Seattle, and change in threat level from orange to red
- Video conference

Issue: Location of NCR Crisis Management Staffs

Observation: Although FEMA has an Interim Operating Facility (IOF) located near the NCR (that is in effect a Federal EOC that is designed to give the Federal Government a location from which to operate and communicate during an emergency), it was not used for this exercise. FEMA and USDHS were correct in believing that the NCR was reacting to a scenario that presented a “credible threat” to the area, although the actual attack was on another part of the country. Both elements of the government would have been operating (at least during this exercise) from their regular offices.

Recommendation: During future NCR exercises, the Federal Government should exercise the IOF so that DC, VA, and MD can gauge any problems they may have in dealing with that specific location (concerning communications, etc). If the IOF had been used for this exercise, the other players (VA, DC, and MD) might have had a better idea of whether they would have trouble communicating with the Federal Government at that location during this type of crisis response/coordination.

Issue: Relationship Between USDHS and FEMA During This Type of Crisis Management

Observation: Although the relationships are still being developed, the new laws and Presidential Directives are quite clear on the relationships and responsibilities of both agencies. USDHS (through the Office of the NCR Coordinator) has policy and Lead Federal Agency (LFA) responsibility for the NCR. FEMA has the same responsibilities that it has always had, and that is to coordinate the Federal response to the consequences of any type of disaster within the region. The only difference is that the USDHS is acting as the LFA on major decisions that are coordinated with the other State-level jurisdictions. It should be noted that both the USDHS and the Federal Coordinating Officer (FCO) for FEMA did an excellent job of coordinating their actions and responsibilities during this exercise. Both Mr. Ken Wall (USDHS) and Mr. Tom Davies (FCO, FEMA) did an outstanding job of fulfilling their roles during this exercise.

Recommendation: The NCR jurisdictions should continue to conduct a wide range of exercises that will prepare and train the entire region in the complex requirements of coordinating all of the government actions required to protect the NCR community from a WMD terrorist attack.

Issue: Change in Threat Level from Yellow to Orange

Observation: The FEMA team took the time to discuss options and actions based on the information regarding the change in threat level, and took the following actions: They simulated calls up their internal chain of command to make recommendations

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

and to seek guidance. They simulated alerting all members of the NCR Emergency Response Team – National (ERT-N) of the change in threat level. The FCO ordered his staff to conduct a communications check with all NCR EOCs. This was actually done at 1:15 p.m., with no prompting. The FCO also had his staff begin keeping a log of all activities.

Recommendation: None. Based on the available information, the FEMA FCO and his staff took proper actions.

Issue: Coordination and Information Sharing Within the NCR

Observation: The first of several NCR conference calls occurred at approximately 1:35 p.m. Participants included the senior leaders of the NCR and FEMA. Available information and intelligence were shared and options for action were discussed and coordinated. In response to an injected fax from USDHS, the FEMA FCO stated that under the circumstances outlined in the scenario, FEMA would be represented in the DC EMA EOC in a real-world setting.

Recommendation: During all future exercises, FEMA representatives in NCR EOCs should be able to act on behalf of their respective organizations (decisionmakers).

Issue: Press Inquiries to FEMA

Observation: The FCO fielded the press inquiries himself; to help ensure a coordinated message, he referred the press to USDHS for comment. This was the correct response both operationally and politically. He clearly understood the importance of a coordinated press release.

Recommendation: Each NCR press officer should continue to develop coordinated NCR media response plans.

Issue: Fax Directing That States Be Informed of Threat Level Change and Specific Actions

Observation: The FCO spoke with his chain of command by phone and recommended that the NCR Management Cell be deployed to the appropriate NCR locations as a precautionary measure. He also recommended that the Region 3 Regional Operations Center (ROC) stand up. He had previously notified all FEMA regions of the change in threat level before being prompted by the fax.

Recommendation: None. All proper actions were implemented.

Issue: Post-Seattle Blast Actions

Observation: The FCO took part in another NCR senior leaders conference call and simulated conversations with his chain of command. He also had conversations with USDHS in which he

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

recommended deployment of the entire NCR ERT-N team. He ordered his staff to ensure that the Continuity of Operations (COOP) site is fully “warm” and that they conduct a communications check with units in the COOP.

Recommendation: None.

Issue: VNN Broadcasts

Observation: Unfortunately, the FEMA representatives taking part in the exercise could not hear the broadcasts because the sound on their PCs did not work, and they did not have control of the volume on the big screen.

Recommendation: Technical support should be available in future exercises to ensure that all participants have the ability to hear what is going on.

Issue: Actions Taken After Seattle RDD Confirmed and Change in Threat Level from Orange to Red

Observation: The FCO, in concert with USDHS and the FEMA chain of command, activated the NCR ERT-N to the emergency relocation site in Maryland. Other pertinent EST activations were also considered so that units would be operational BEFORE an event occurred in the NCR. FEMA operations would have moved to their IOF so as to be out of the DC area prior to an event. FEMA regions and NCR EOCs were kept apprised of actions taken by FEMA.

Issue: Video Conference

Observation: FEMA representatives were unable to access video conferencing during the exercise due to technical problems. The FCO instructed his staff to ensure that all necessary names and phone numbers of points of contact (POCs) are available for real emergencies. He stated that in the real world, he would have had the technical support he needed to take part in the video conference.

Recommendation: Proper video communications support should be made available to all key NCR facilities before the next scheduled NCR exercise.

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

**DISTRICT OF COLUMBIA EMERGENCY MANAGEMENT AGENCY
EMERGENCY OPERATIONS CENTER
WASHINGTON, DC**

General Statement

The District of Columbia Government and EMA worked collectively with several other EOCs to exercise their plans. This exercise proved to be beneficial to the DC government and the DC EMA. The DC EMA stood up all Emergency Support Functions (ESFs), even though a few agencies either reported late or failed to report.



The controllers witnessed DC EOC participants working very well with each other and within their respective ESFs. Information was passed among agencies in a proper and respectful manner. Most of the participants understood and performed their roles in the DC EOC. These same participants carried out their responsibilities as they were instructed and as they had practiced in previous training exercises.

In the beginning of the exercise, the leaders of the DC EOC appeared to be somewhat loose with the management of the operations. As the exercise progressed, they gained and maintained control of the exercise EOC staff. The only recommendation that can be offered is to practice, practice, and practice.

Specific issues identified at the District of Columbia EOC:

- Unfamiliarity of the new E-Team Software
- Technical Issues
- Security
- Public Information
- Reports from ESFs



Issue: Lack of Familiarity With New E-Team Software

Observation: Several of the participants in the DC EOC appeared to be having difficulty using this software, at least in the beginning of the exercise. Prior to the start of the exercise, a special training session on using the new software was held in the EOC. Not all participants in the DC EOC were present for this training.

Recommendation: Training for participants who will use this software in the future should have been held several days before the exercise. The DC Information Technology section provided several staff members to assist with questions and problems as they arose. The

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

participants should have been given more time to learn and experience the advantages of the software prior to using it during a real or simulated terrorism event.

Issue: Technical Issues

Observation: Many participants were forced to wait for data from EOC printers. In many cases, this is a trivial issue. During this exercise, however, many participants were waiting for printed copies in the area where the Operations Chief and his staff were trying to manage the situation. People standing in this area tended to cause several problems: obscuring the Operations Chief's ability to see the participants and the information displayed on the video screen(s); distracting the Operations Chief and/or his staff by the conversations being held; and the ability of other participants to move freely through the DC EOC to gather information.

Recommendation: There should be more than one printer for 45 workers in the DC EOC. This printer(s) should be located close to the ESF areas without obscuring the vision of the Operations Chief and/or staff, and where they will not interfere with the flow of traffic through the DC EOC.

Issue: Security

Observation: During the exercise, many observers passed through the main area of the DC EOC. The majority of these observers were local dignitaries and/or VIPs of the DC Government. The process for checking the identification of all persons entering the EOC appeared to be in place, but many of the visitors were not checked against an "authorized access" list.

Recommendation: Implement a more visible method of indicating that security checks were performed and a person has been cleared to enter the sensitive area. The liaisons for each of the ESFs should be able to quickly determine if a person/observer has the proper credentials to be in the EOC. This ensures safe operations of each ESF Liaison.

Issue: Public Information

Observation: The DC EMA public information officer (PIO) and staff appeared to be very busy dealing with the visiting dignitaries. Their participation in the exercise appeared to be minimal.

Recommendation: It is understood that when a real-world situation is unfolding in the DC EOC, the visitors will not be in the DC EOC. This should free the PIO and her staff to perform those duties as identified in the DC EOC protocols.

DC EOC needs to identify a location where joint regional information can be obtained and verified, briefings can be developed, and contacts can be directed regarding the event(s). The contact information and location of this Joint Information Center (JIC) should be provided to all participants in the DC EOC and the surrounding EOCs. Information to the public and the news media regarding the safety of the public is very critical during an incident.

DRAFT

Recommendation: Three methods could be implemented to deal with this observation. First, develop a template of what information needs to be reported by each ESF; second, through analysis of past exercises, determine which ESFs need to report during a particular work period(s)—develop a checklist to help the DC EMA Operations Chief and/or his staff to manage these reports. Third, set timeframes for the presentation of the ESF reports, and have the ESFs practice making reports in that timeframe.

National Capital Region Functional Exercise After-Action Report

**FEDERAL BUREAU OF INVESTIGATION
WASHINGTON FIELD OFFICE
WASHINGTON, DC**

General Statement

For pragmatic reasons, the participation of the NCR in any TOPOFF exercise is indispensable. In any incident, whether natural or man-made, the resources of the Federal Government will require some time to respond and arrive at the scene of an incident. These resources, in the form of personnel and assets, are critical to the preservation of life and the restoration of important infrastructure. This is particularly true when the incident(s) involves terrorists and the use of WMD.

An exercise of the magnitude of T2, with the participation of thousands of individuals (elected and appointed; State, county, and municipal; crisis and consequence responders), jurisdictions within the continental United States, and international implications, necessitates the consideration and active involvement of the NCR. The NCR is the keystone to most if not all of the Nation's central databases; it serves as the conduit for national, regional, State, and local representation and decision-making; it is positioned to activate and dispatch specialized personnel and vital assets to affected areas; it is central in the gathering and dissemination of information and intelligence throughout the United States and internationally; and as the seat of national government and host to commercial associations, nongovernmental organizations, and countless other entities, the NCR is directly or indirectly impacted by events that occur anywhere in the United States and its territories, and even in other countries. Therefore, the NCR should be integral in all aspects of the TOPOFF exercises.

The participation of the NCR in T2 was not integral and its presence was an afterthought, which short-circuited many of the operational procedures that normally take place. The results were confusion, miscommunication, misdirection, and ineffective action. The participation of the FBI WFO is a case in point. It was tasked with the role of performing and executing functions that are not within its normal realm, which contributed to actions inconsistent with proper procedures. As expected, this resulted in questioning of the value of the exercise.

In addition to the pragmatic reasons for NCR involvement, there are also symbolic reasons, such as conveying the command and control of the government by representative leadership. The functioning of the government's departments and agencies is a statement of the stability of the government.

Specific issues identified at the FBI WFO:

- National exercise participation
- Generation of exercise intelligence
- Communications and intelligence release

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

Issue: National Exercise Participation

Observation: The NCRFE was based on the events of T2, but NCRFE participants were not permitted to intermingle with T2 players. Due to the very nature of the NCRFE, participating agencies raised questions and concerns regarding T2 events and intelligence generated at the Seattle, WA, Incident Command. Because additional exercise information was not available, the FBI WFO was forced to break with NCRFE communication protocols and contact the Strategic Information and Operations Center (SIOC) regarding Seattle incident intelligence, and pass this information on to all participating agencies.

Recommendation: FBI WFO, National Capital Response Squad (NCRS), recommends that future National Field Training Exercises (FTXs) have either the full participation of all agencies involved without limits on communications, or no participation at all in the FTX. Limiting agencies' participation is counterproductive and unrealistic during a true WMD event.

Issue: Generation of Exercise Intelligence

Observation: A raw intelligence product was developed for the T2 exercise and provided to the WFO FBI as part of the NCRFE. WFO was participating as both FBI HQ/SIOC and the FBI Field Office, and did not have sufficient time to generate a working intelligence product to release as exercise intelligence for the initiation of the NCRFE.

Recommendation: Increased preparation time for FBI analysts would allow for generation of a useful intelligence product. This product could then be disseminated to relevant State and local agencies for use in asset deployment and event evaluation.

Issue: Communications and Intelligence Release

Observation: Communication among exercise controllers and the release of exercise intelligence needs to be re-evaluated. Allowing the intelligence products to control the exercise actions is a realistic scenario. However, by providing all NCRFE participating agencies with the same intelligence product at the same time through exercise controllers defeats the nature and objectives of the NCRFE exercise. Appraising the command and control issues among the various agencies is nullified by this action.

Recommendation: FBI WFO NCRS recommends that the agency responsible for generating the intelligence should control the product and disseminate the information accordingly.

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

MARYLAND EMERGENCY MANAGEMENT AGENCY (MEMA)
EMERGENCY OPERATIONS CENTER
REISTERSTOWN, MD

General Statement

As part of the NCRFE, MEMA sought to evaluate its own processes and capabilities while engaged in a simulated domestic security incident of significant scope. Representatives from various relevant Maryland agencies were present, and the participation level from all players was high.



Representatives from the State of Maryland participated in the exercise primarily from a conference room area located within the State of Maryland EOC, and all injects were received there and disseminated to the participants around the table for discussion. This design led to a cooperative information-sharing environment and was a benefit to the exercise participants. The State of Maryland was also able to use a secure video conference capability that was shared with DC and VA, which would have been critical for any necessary secure teleconferences. Unfortunately, due to technical problems with some outside systems, the video interface was minimal. However, the Maryland EOC was able to receive the VNN live feeds that originated from the State of Washington, which was invaluable for information acquisition, enhancing the exercise as a whole.

The State of Maryland participated to the fullest extent in a highly effective functional exercise environment, and some very significant issues were brought to the surface throughout the day.

Specific issues identified at the Maryland Emergency Operations Center:

- Regionalized domestic security threat condition change
- Information sharing among the NCR jurisdictions
- “Essential Employee” designation

Issue: Regionalized Domestic Security Threat Condition Change

Observation: A critical issue of concern that Maryland had throughout the NCR exercise dealt with the shifting of domestic security threat level conditions. Questions arose from the State about whether it was a USDHS requirement for Maryland to issue a statewide threat condition elevation, or whether that threat condition could be elevated regionally, i.e., affecting only the NCR jurisdictions. Maryland stated that a series of required security and legislative protocols would be put into effect if the domestic security threat level condition is raised to red, and that the State should have the ability to regionalize the threat level elevation to include the areas of highest vulnerability, but not be so inclusive as to prohibit “normal” operations statewide in

areas of lesser vulnerability. Maryland did recognize through its discussions that there is a distinct liability issue, as well as a reliance on other jurisdictions and cooperative efforts, that exist within the NCR jurisdictions. Decisions for the State of Maryland would not be made without, at the very least, consultation with the DC and VA.

Recommendation: It was clear that this issue needs to be examined further. Consider a collaborative panel discussion or workshop with representatives from the NCR jurisdictions; the State of Maryland; the State of Virginia; the District of Columbia; USDHS; and other relevant regional and Federal partners and stakeholders, with regionalized domestic security threat level condition change as the principal subject for discussion.

Issue: Information Sharing Among the NCR Jurisdictions

Observation: During the NCRFE, there was a minimal level of information sharing and collaboration among the NCR jurisdictions within the allocated response timeline presented in the scenario. The sharing of information was primarily done through pre-scheduled conference calls in which all relevant jurisdictions and Federal agencies participated. The conference calls were facilitated by USDHS and primarily dealt with global issues relevant to all involved. There was very little independent information sharing that took place outside of the conference call format. The State of Maryland struggled with some critical issues throughout the afternoon that were presented to them as a result of the exercise events. Similar issues were likely encountered within the other participating NCR jurisdictions as well, but at no time outside of the pre-arranged conference calls was DC or VA queried as to how they were handling these issues of concern. This observation goes both ways: neither NCR jurisdiction reached out to the State of Maryland to discuss situations or share information during the exercise. As critical regional partners, the sharing of information is essential to a coordinated and effective response.

Recommendation: Continue to foster a regional relationship with DC and VA as NCR partners through exercises and training such as the NCRFE. Continued collaboration and partnership in training, exercises, and plan development only enhances the NCR's overall level of domestic preparedness.

Issue: "Essential Employee" Designation

Observation: There was a great deal of discussion among players about Maryland's current "essential employees" list. This list was designed to address the State's critical employee needs in the event of an emergency triggered by a natural disaster. It lists those employees who would be required to report to work despite a situation that would warrant the closing of government offices. Players noted that this list may not accurately reflect the State's employee requirements in the event of a domestic security threat or act of terrorism. There was some discussion as to how this situation could or should be resolved. Also, players discussed how, exactly, such an order would be carried out on a statewide basis. That is, would a domestic security disturbance in the Washington, DC, or Annapolis area necessitate the closing of government offices in other regions? The question remains: how should the recommendation be written to reflect these

National Capital Region Functional Exercise

Anything that can be clarified immediately, however, should be. For example, a clear understanding needs to be reached between the Federal Government and Maryland as to what employee expenses, if any, are reimbursable. This is a particularly acute problem if there is an expectation that all NCR jurisdictions will react to the same threats in the same manner.

National Capital Region Functional Exercise

DRAFT After-Action Report DRAFT

U.S. DEPARTMENT OF HOMELAND SECURITY
NATIONAL CAPITAL REGION
WASHINGTON, DC

General Statement

The USDHS, ONCRC was actively involved in the exercise and participated in their role in providing policy guidance and coordination for the NCR jurisdictions. This aspect of the exercise went very smoothly.

Unfortunately, the actual NCR Coordinator was detailed to Seattle for T2, so his deputy participated in the exercise and did a great job. In the future, it might be beneficial for all principals to participate in these types of exercises.

The Deputy NCR Coordinator operated out of his office, as this is where he would begin during an actual incident until the time that the Federal agencies' relocation sites were activated. In future exercises it would be beneficial to take the scenario to the point where these sites are activated so that agencies can adequately assess how this process will occur, as well as the ability to effectively communicate with one another.

Specific issues identified at the USDHS:

- Coordination and Policy Guidance
- Communication and Coordination with Other NCR Jurisdictions

Issue: Coordination and Policy Guidance

Observation: Providing policy guidance and coordination for the National Capital Region is a new role for the U.S. Department of Homeland Security, and it was accomplished without any problems. The Deputy Coordinator has a good understanding of what actions he needed to take in order to provide the necessary information to the NCR jurisdictions.

Recommendation: Conduct more NCR response exercises to further improve new working relationships.

Issue: Communication and Coordination with Other NCR Jurisdictions

Observation: The Deputy Coordinator was actively involved in all conference calls that took place during the course of the exercise between the Federal agencies and the NCR jurisdictions.

Recommendation: As noted by the Maryland EOC evaluator, more direct communications between NCR jurisdictions is needed in future NCR exercises.

APPENDIX A
EXERCISE PARTICIPANTS

DC EOC

(b)(6) DC WASA
(b)(6) DC WASA
(b)(6) USSS
(b)(6) G.U.
(b)(6) G.U.
(b)(6) G.U.
(b)(6) G. U.
(b)(6) G.U.
(b)(6) DC O.C.T.O.
(b)(6) DC WASA
(b)(6) MDW
(b)(6) DC Hospital Association
(b)(6) DC DPW
(b)(6) DC DPW
(b)(6) DC FO
(b)(6) DC FO
(b)(6) HAWDC
Ghermay Aranga, O.C.T.O.
(b)(6) DC Fire
(b)(6) O.C.T.O.
(b)(6) GWU
(b)(6) DCMA
G. Bryan Jones, DHS/PHS Region III
(b)(6) EMA
(b)(6) OPM OSKA
(b)(6) OCP/PSC
(b)(6) PEPCO
(b)(6) FPS-DHS
(b)(6) MPD-SOD
(b)(6) USCP
(b)(6) DDOT
(b)(6) O.C.T.O.
(b)(6) DDOT
(b)(6) DCNG
(b)(6) DC WASA
(b)(6) DC WASA

MD EOC

Don Keldsen, MEMA

(b)(6) DHMH
(b)(6) MEMA
(b)(6) MIEMSS
(b)(6) MSP
(b)(6) MSP
(b)(6) MDE
(b)(6) MEMA
(b)(6) MEMA
(b)(6) MEMA
(b)(6) MEMA
(b)(6)
(b)(6) MSP
(b)(6) City of Annapolis
(b)(6) MEMA
(b)(6) MEMA
(b)(6) DHMH
(b)(6) MDOT
(b)(6) DHMH
(b)(6) DHMH
(b)(6) MIEMSS

VA EOC

(b)(6) VDEM
(b)(6) VDEM
(b)(6) VDEM
Dawn Eischen, VDEM
(b)(6) VDEM
(b)(6) VDEM

FBI-WFO

(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI

TOP OFFICIALS (TOPOFF) EXERCISE SERIES:

TOPOFF 2 (T2) After Action Report ANNEX D



September 30, 2003

Information contained in this document is intended for the exclusive use of T2 Exercise Series participants. Material may not be reproduced, copied, or furnished to non-exercise personnel without written approval from the Exercise Directors.

This page intentionally left

For Official Use Only



TOPOFF2 CYBEREX

AFTER ACTION REPORT

JULY 2003



**INSTITUTE FOR SECURITY TECHNOLOGIES AT
DARTMOUTH COLLEGE**

For Official Use Only

TOPOFF2 Cyberex – After Action Report

TOPOFF2 AAR #041

Copyright (c), 2003, Trustees of Dartmouth College (Institute for Security Technology Studies). All rights Reserved. Supported under Award number 2000-DT-CX-K001 from the Office for Domestic Preparedness, Department of Homeland Security. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security.

For Official Use Only

TOPOFF2 Cyberex – After Action Report

TABLE OF CONTENTS

Section	Page
1 Executive Summary	1-1
2 Tasking	2-1
3 Stakeholders	3-1
4 Seminars	4-1
5 Simulation	5-1
6 Exercise Design	6-1
7 Game Play	7-1
8 Observations	8-1
9 Recommendations for TOPOFF3	9-1
Appendix	
A Problem Chains	A-1
B Master Scenario Event Listing (MSEL)	B-1
C Sample Simulation Communications Output	C-1
D Press Release	D-1

For Official Use Only

TOPOFF2 Cyberex – After Action Report

TOPOFF2 CYBEREX

EXECUTIVE SUMMARY

The national infrastructure of the United States is vulnerable to disruption by physical attack because of its interdependent nature and by cyber-attack because of its dependence on computer networks. Those who intend to do harm to the United States will seek to exploit vulnerabilities using conventional munitions, weapons of mass destruction (WMD), and cyber-weapons. Over time, such attacks are increasingly likely to be delivered through computer networks rather than using conventional munitions alone, as the attractiveness of cyber-attacks and the skill of U.S. adversaries in employing them evolve. Cyber-attacks will provide both state and non-state adversaries with new options for action against the United States beyond mere words.

TOPOFF2 is the second Congressionally mandated, counter-terrorism exercise involving senior U.S. government officials, multiple Federal / State / Local agencies, and Canadian government agencies. The goals of TOPOFF2 were to improve the nation's capacity to manage extreme events; create broader operating frameworks of expert crisis and consequence management systems; validate authorities, strategies, plans, policies, procedures, and protocols; and build a sustainable, systematic national exercise program to support the national strategy for homeland security. While traditional crisis and consequence management organizations were the principal foci of TOPOFF2, there exists another element of our country's critical infrastructure that experts consider highly vulnerable to terrorist-related attack: the national information infrastructure.

TOPOFF2 CYBEREX was a functional exercise to examine, in an operational context, the integration of inter- and intra-governmental actions related to a large-scale cyber-attack synchronized with a terrorist WMD attack against a major urban area of the United States. In the course of these proceedings, players addressed those actions needed to limit the potential damage caused by network compromise and to minimize the impact on operations resulting from the loss of these resources. While exploring the vast complexities of these individual and inter-related actions, this exercise provided an opportunity for

For Official Use Only

TOPOFF2 Cyberex – After Action Report

decision-makers and staffs to identify, discuss, and resolve critical issues associated with a cyber-attack and other significant disruptions to their network infrastructures. During these activities players explored potential vulnerabilities and anticipated responses to determine if and what changes might be necessary to existing cyber-security programs and organized responses. Approximately 125 people participated in the exercise on the 6th and 7th of May, 2003. The exercise was held at the Washington State Emergency Operations Center in Camp Murray, Washington.

Lessons Learned:

Participants saw value in a regionally coordinated cyber-security efforts-- in timely exchange information and collective response. The development of this regional approach between State and Local government agencies that participated in TOPOFF 2 will continue post exercise.

The exercise highlighted a need to examine how cyber-response plans and procedures correspond to changes of the color-coded national threat condition promulgated by the Department of Homeland Security (DHS). From a cyber-perspective, what proactive steps should be taken when the threat condition escalates from yellow to orange and then to red? The players examined these and other similar questions.

There are no formally established processes, similar to those in place for a physical attack or natural disaster, that address coordination between the federal government and its state and local counterparts in the event of a cyber-attack

The ability to maintain information technology (IT) infrastructure is predicated on the fact that individuals will be able to get to their workspace. In those instances where this is not true, government agencies responsible for IT infrastructure should examine how they would perform mission-critical functions such as backups and systems maintenance from alternate locations.

~~For Official Use Only~~

TOPOFF2 Cyberex – After Action Report

During the pre-exercise period, federal government agencies responsible for infrastructure protection were not yet completely evolved due to the stand-up of the new Department of Homeland Security. The federal government should develop an integrated cyber-response plan that addresses crisis support to both state and local governments. There is a need for a single point of direct contact between the federal government and State and Local governments for dissemination of information related to cyber-attacks.

T2 AAR #041

For Official Use Only

TOPOFF2 Cyberex – After Action Report

SECTION TWO:

TASKING

INTRODUCTION

The Institute for Security Technology Studies at Dartmouth College (ISTS) is a federally funded Institute which was founded in the FY 2000 appropriation as a national center for counterterrorism and cyber-security R&D. Our mission is to work to secure computer networks against attack, enhance Law Enforcement investigative capabilities in cyber-crimes, and serve as a center for counterterrorism technology research, development, testing, and evaluation. To accomplish this goal we have over 70 researchers at Dartmouth College and employ 20 researchers from other institutes working on research projects related to this mission.

Funding for the ISTS at Dartmouth College was supported under Award number 2000-DT-CX-K001 (S-2) from the Office of Justice Programs, National Institute of Justice, Department of Justice.

The Office of Domestic Preparedness (ODP) had decided after TOPOFF 2000 that TOPOFF II should include a cyber-component. Representatives from ODP met with the Director of the ISTS at Dartmouth College early in 2002 and the two organizations agreed that the ISTS should take a lead role in preparation and conduct of a cyber-exercise for TOPOFF II. Not only does this task align with the mission of the ISTS, but this relationship ensured that the ISTS could provide funding necessary to conduct the cyber-exercise for TOPOFF II at no cost to ODP, a necessary condition for completion of the project on schedule.

For Official Use Only

TOPOFF2 Cyberex – After Action Report

SECTION THREE

STAKEHOLDERS

PRINCIPAL STAKEHOLDERS

TOPOFF2 CYBEREX players were primarily those Federal, State, County, City, private sector, and personnel from the Government of Canada who have active roles in the daily operations, management, and security of their information networks, systems, or infrastructure within their organizations. These participants would most likely play key roles in responding to or managing the consequences of a significant regional cyber-disruption or attack. The principal stakeholders in the exercise were:

- IT organizations and Top Officials from:
 - Washington State
 - King County
 - City of Seattle

Supporting these players were representatives from the following organizations:

- A commercial telecom provider and local Internet Service Provider (ISP)
- Federal computer incident response agencies
- Federal law enforcement agencies

ORGANIZATION AND ROLES

The following is a summary of the organizations involved in the exercise.

- Five Network Operation Centers (NOCs) participated in this exercise:
 - City of Seattle
 - King County
 - Washington State Department of Information Services (DIS)
 - Washington State Department of Transportation (DOT)

For Official Use Only

TOPOFF2 Cyberex – After Action Report

- Washington State Emergency Management Department (EMD)

Each exercise NOC was composed of individuals from within the organization who are assigned to these NOCs on a routine basis. These groups responded to and managed consequences presented in the exercise. Because of the restricted time available during the exercise, not all elements of an organization's response were addressed. Unresolved issues necessary to keep a NOC's actions and deliberations flowing were resolved by a group's facilitator or the Control Team and brought forward during the final plenary session. The general responsibilities of the NOCs included:

- Assessing network status.
 - Exploring the impact of differing proactive response strategies.
 - Responding to network disruptions.
 - Providing periodic summaries to Top Officials (TOPOFFs).
 - Developing recommendations for TOPOFFs.
 - Sharing information with other NOCs.
 - Sharing resources with other NOC's.
 - Responding to mock media inquiries.
- A group of Top Officials from Federal, State, County, and City government organizations participated in TOPOFF2 CYBEREX. In addition to observing exercise activity and assessing their ability to work as a team, these officials acted as an executive body to address and resolve cyber-security issues challenging the NOCs. These senior executives were incorporated into the TOPOFF Coordination and Communication Group (TCCG). The function of the TCCG was to provide a forum for senior executives to:
 - Gain and maintain situational awareness of emerging events, develop strategic courses of action to conduct a concurrent and integrated response, and direct appropriate actions.
 - Mitigate consequences of enterprise network disruption or loss.
 - Address and resolve the allocation of limited resources among competing demands.

For Official Use Only

TOPOFF2 Cyberex – After Action Report

- Collect, analyze, formulate, and disseminate information to stakeholders in and outside the state, including the media.
- Develop recommendations for political leadership (chief executive) approval or action.
- Respond to inquiries from senior executives of the Federal government.

Accordingly, to work effectively in an inter-governmental environment, the Top Officials from each organization assigned to the TCCG had experience, authority, and access to the organization's political leadership. Chief information / chief technology officers (CIO / CTO) and/or members of their immediate staffs filled these positions during the exercise. Top Officials came from the following organizations:

- State of Washington CIO / Director of Washington State DIS
- State DOT (Information Technology Section)
- State EMD (Telecommunications Section / Director's Office) and National Guard
- Office of the Governor
- King County (Information and Telecommunications Services Division / Office of Information Resource Management)
- City of Seattle (Department of Information Technology)
- University of Washington (University Computing Services)
- Top Officials played by the Control Team:
 - Governor
 - County Executive
 - Mayor
 - Department of Homeland Security (DHS)

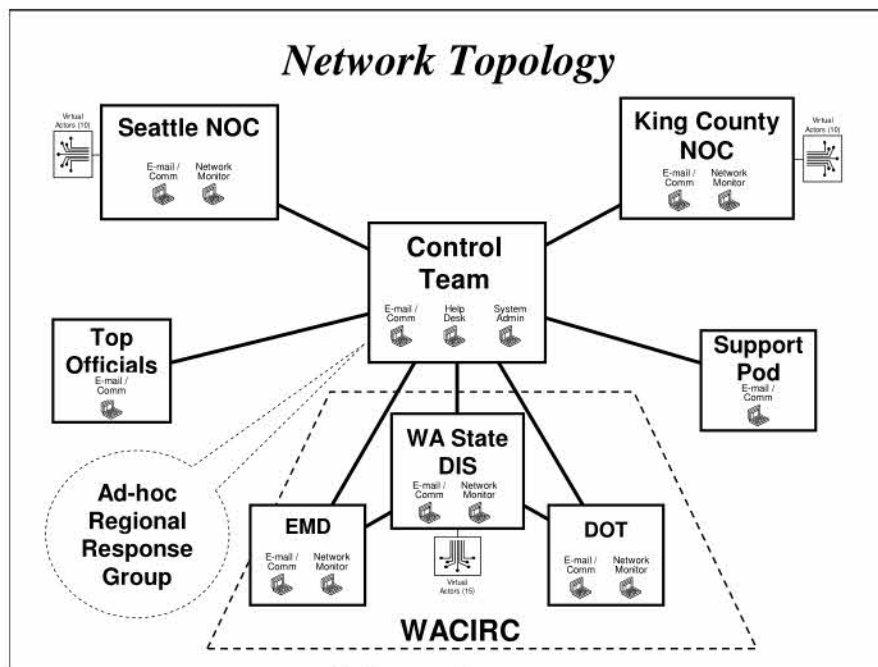
Another group, acting in support of the TCCG, consisted of regional government and corporate representatives who would have a logical role to play given the scenarios. Unlike the NOCs and the TCCG, the Support Pod had no direct "play" in TOPOFF2 CYBEREX. Rather, their role was to provide information to, and respond to resource requests from, the principal players. Representatives of support organizations had an in-depth understanding of the

For Official Use Only

TOPOFF2 Cyberex – After Action Report

technologies, capabilities, and processes that their organization would provide the principal players, and the methodologies to avail these resources.

The following diagram depicts the overall organization of TOPOFF2 CYBEREX.



EXERCISE OBJECTIVES

TOPOFF2 requirements stated that: "This series of exercise components will also improve 'crisis resistance' through opportunities to measure plans, policies, and procedures required to provide an effective response to a weapons of mass destruction (WMD) terrorist incident." This type of incident would be more complex and significantly challenge the capabilities of organizations assigned the responsibility of providing a first response if government-related information networks were simultaneously and maliciously disrupted due to a large-scale cyber-attack. Accordingly, within the context of a TOPOFF2-like WMD event, the players gave due consideration to the following issues and objectives during the development of the CYBEREX:

For Official Use Only

TOPOFF2 Cyberex – After Action Report

- The effectiveness of the various cyber-security plans, policies and procedures of the City, County, State, and Federal levels to adequately address issues and support the response for a large-scale cyber-attack on government-related information networks.
- The ability of participating NOCs to organizationally integrate and effectively conduct or manage a sustained response to a cyber-attack.
- The planned flow of communications and information in an operational context.
- The decision and coordination processes in a range of potential consequences.

Within these overarching set of objectives, each of the principal stakeholders had their own objectives for this exercise. These included:

- DIS - Determine that the Washington State Computer Incident Response Center (WACIRC) procedures -- including incident reporting, response, escalation, communications, containment, etc. -- were sufficient to effectively mitigate the effects of cyber-attacks.
- City of Seattle & King County - Develop policies and procedures relating to large-scale cyber-attacks, including federal notification and response.
- City of Seattle & King County - Determine the effectiveness of the draft policies and procedures along with federal notification procedures.

Throughout the development of the exercise, these objectives guided the design and methodologies used to achieve the stakeholders expectations. A flexible design structure was used for the development of this exercise, thus allowing for the incorporation of new objectives should they arise.

It became apparent during the design of the game that the principal stakeholders realized that there might be significant value in developing a regional approach to a response to a major cyber-attack. The stakeholders held several meetings to address this regional approach to the problem. One outcome of these discussions was the proposal for a regional information sharing system to be used by the stakeholders to report significant anomalies occurring on each organization's networks. This prototype system, entitled the Regional Information and Intelligence Gathering (RIIG) was exercised in the two-day event. Additional refinement on this initiative was planned after the exercise based on how the RIIG was used during the event.

For Official Use Only

TOPOFF2 Cyberex – After Action Report

Additionally, this exercise was designed so that principal stakeholders may develop strategies and planning frameworks to:

- Coordinate inter-governmental responses and consequence management to cyber-attacks.
- Maintain continuity of operations within participating organizations.
- Develop alternatives and recommendations to senior or executive decision-makers in responding to potential cyber-crisis events.
- Sustain confidence in government information networks during a cyber-attack and, if necessary, regain public confidence.

Each participating organization developed its own self-evaluation criteria for the exercise. Inclusion of these criteria and the results of their assessment go beyond the scope of this report. Here we address information and resources sharing between organizations.

The following is a summary of the organizations participating in TOPOFF2 CYBEREX:

King County

- Department of Executive Services
- Department of Natural Resources and Parks
- Department of Public Health
- Department of Transportation
- Information and Telecommunications Services Division
- Office of Emergency Management
- Prosecuting Attorney's Office
- Sheriff's Office
- Department of Transportation
- Police Department
- Seattle Center
- Seattle City Light
- Seattle Public Utilities

City of Seattle

- Department of Information Technology

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

Washington State

- DIS
- DOT
- EMD
- Office of the Governor

Canada

- Office of Critical Infrastructure and Emergency Preparedness
- Province of British Columbia Ministry of Management Services
- Province of Ontario Information Protection Center

Other Participants

- Boeing Corporation
- Federal Bureau of Investigation – Seattle office
- CERT at Carnegie Melon
- National Communication System
- Microsoft Corporation
- Qwest Corporation
- United States DHS
- United States Department of State
- United States Secret Service – Seattle Office
- United States Attorney
- University of Washington

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

SECTION FOUR

SEMINARS

As part of the exercise development and learning process for the stakeholders, we held two seminars in the Seattle area at the Criminal Justice Training Center. Each was attended by about 125 people from the stakeholder community including State of Washington, King County, and City of Seattle's government agencies. Representatives from the Port of Seattle, Boeing, Microsoft and the University of Washington also attended. The seminars were held at no cost to the participants. In general, presenters donated their time and travel expense.

Seminar 1: Notification Policies Seminar – to review areas of responsibilities of federal agencies, reporting thresholds, trigger points to access resources, and escalation procedures.

- Held 6 February, 2003.
- Moderator: (b)(6) former Director of the Department of Defense Cyber Crime Center.
- Presenters
 - (b)(6) – NIPC
 - (b)(6) – FBI, Seattle
 - (b)(6) – USSS, Seattle
 - (b)(6) – US Attorney's Office
 - (b)(6) – National Communications System
 - (b)(6) – Qwest
 - (b)(6) and (b)(6) – OCIEP of Canada
 - (b)(6) – ISTS-Dartmouth College on the recent Slammer Worm

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

Seminar 2: Threat Assessment Seminar – What are the threats, what are the tools we have to defend against them, how do we conduct a cost benefit analysis to determine which tools to invest in?.

- Held: 11 March 2003
- Moderator: Dr. (b)(6) CIA Senior Scientist - Info Ops Center
- Presenters:
 - Dr. (b)(6) – National Security Council, Office of Cyberspace Security
 - (b)(6) – ISTS at Dartmouth College – end effects and methods
 - (b)(6) – CERT
 - (b)(6) – NIPC Unclass Threat Assessment
 - (b)(6) – University of Washington
 - (b)(6) – City of Seattle CISO and founder of Agora
 - (b)(6) – Defense in Depth

SECTION FIVE

SIMULATION

As the CYBEREX portion of TOPOFF2 was conducted on a not-to-interfere basis with the principal exercise, the network operation centers (NOCs) of participating organizations employed a simulated network, developed by the Institute for Security Technology Studies (ISTS) at Dartmouth College as a primary source of exercise-related stimuli.

This simulated network replicated the functional elements of regional wide area networks, inter-governmental networks, and access to the public Internet. Exercise designers worked with network managers of participating organizations to develop a plausible emulation of the organizations' networks, while ensuring that the simulation did not reveal critical vulnerabilities or disclose exact security measures. Participants had final approval on the network simulation used by their organization during operational exercise activity. The below diagram depicts a simulated network display used by one of the stakeholders:



For Official Use Only

TOPOFF2 CYBEREX – After Action Report

Employing a Master Scenario Event Listing (MSEL) developed before the exercise with the assistance of stakeholder Trusted Agents, simulation controllers were able to generate disruptions to simulated network hardware, such as workstations, routers, firewalls, servers, and to the connectivity “pipes” connecting them. These controlled disruptions were based on actions of the attacking agents and included malicious events and normal disruptions. The effects of these disruptions were revealed to the players on a Web-based display application that highlighted the location of the disruption and often its severity. Remediation of these problems was made through player interaction with members of the network control team. Details of the MSEL are included as an appendix to this report.

In addition to stimuli being provided by the network simulation, participants received injects through an exercise communication system developed for the CYBEREX. From a single computer workstation, participants could send and receive e-mail and replicate the use of telephone, facsimile or pager systems.

Before interactive play of the exercise began, operators of the network status display consoles were indoctrinated on its use. A briefing of this network was also provided to participants as part of the opening orientation session.

For Official Use Only

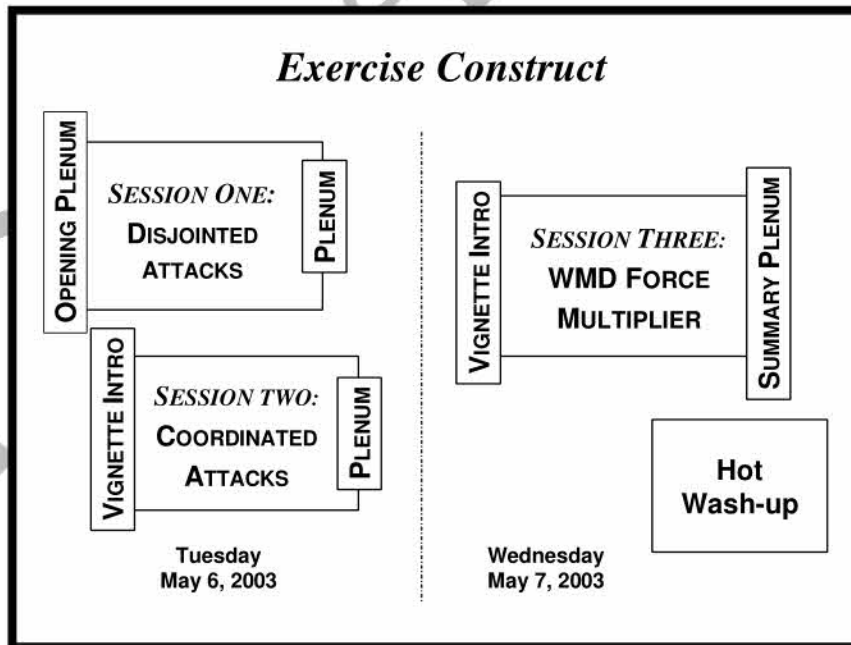
TOPOFF2 CYBEREX – After Action Report

SECTION SIX

EXERCISE DESIGN

CONCEPT OF EXERCISE ACTIVITY

TOPOFF2 CYBEREX was a facilitated, computer assisted, one and one-half day, immersive, scenario-supported, and network-aided interactive exercise where executives and staffs of governmental information technology (IT) organizations explored the challenges of managing disruptions to critical computer networks caused by a terrorist cyber-attack. Participant activity was centered on three vignettes, each associated with different aspects of the complex cyber-security problem. The successive vignettes represented escalating levels of attack and stress for the players. The attacks simulated during the exercise were designed to expose players to a series of exploits which have all been seen in the wild, but which they themselves may never have seen before. The following diagram depicts the construct and flow of these vignettes:



For Official Use Only

TOPOFF2 CYBEREX – After Action Report

The following is a brief description of each vignette.

- **Vignette One:** Sporadic attacks that affect the State, County, and City network operations. These attacks were not to occur simultaneously, and appeared somewhat disjointed. The intensity of the attacks represented an above-normal level of malicious activity.
- **Vignette Two: Coordinated** attacks of longer duration that reflected multiple attack methodologies. Attack intensity corresponded to the high-end of normal malicious activity and was intended to cause minor to moderate disruption of government information networks.
- **Vignette Three:** Attack coincident with the weapons of mass destruction (WMD) event that **incorporated** the gamut of public-knowledge attack methods. This compound attack was intended to be a “force multiplier” of the WMD event and was directed at specific networked entities with crisis or consequence management roles.

A Hot Wash-up concluded the interactive portion of this exercise. Each group presented the significant and unresolved planning and management concerns, critical issues, and recommendations identified in each session.

First and foremost: **This exercise was not a test.** Rather, it was an opportunity for participating organizations and individuals to stress their plans, policies or procedures, improve coordination and confidence, augment skills, refine roles and responsibilities, reveal weaknesses and resource gaps, and build teamwork.

Although the incident management and cyber-security plans used by participating organizations provided a foundation for players’ actions, these actions and decisions were not constrained by these plans or other current, real-world plans and management concepts.

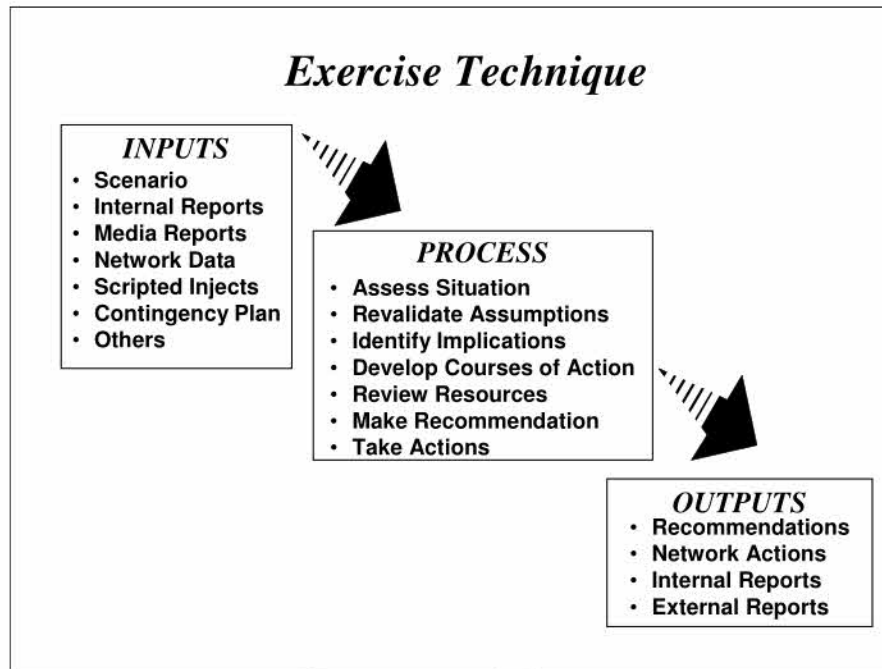
EXERCISE TECHNIQUE

The overall technique employed for this exercise was based on an input ⇒ action ⇒ output paradigm. Using information provided by a scenario, injects, or network status displays,

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

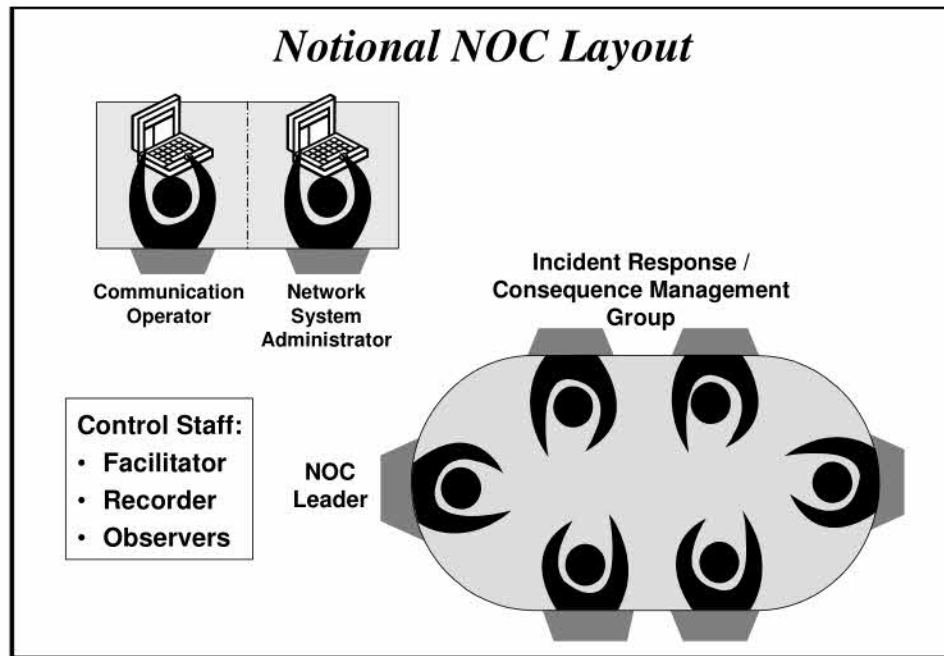
participants responded to issues related to a vignette. Facilitators assigned to each group assisted the participants through the exercise process and discussions. The following depicts the general flow of this interactive technique:



For Official Use Only

TOPOFF2 CYBEREX – After Action Report

The principal organizational structure for each stakeholder was a Network Operations Center (NOC). The diagram below provides a notional layout of an organization's NOC:



Each NOC had three primary entities:

- Network Systems Administrator (NSA)
- Incident Response / Consequence Management Group (IR / CMG)
- Communications Operator

The following discussion details the roles and responsibilities of members of the NOC.

- **Network System Administrator (NSA):**

Using data and information provided from a computer display, the NSA was responsible for monitoring the network, and identifying, documenting, and recommending solutions to problems discovered. Additionally, the NSA took actions, within his / her authority, to respond

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

to the network situation. The NSA also performed network systems troubleshooting to isolate and diagnose system problems. This individual was experienced with the organization's network topology and NSA procedures. Additionally, the NSA possessed an understanding of the underlying technology behind the hardware operating the network and the principal software applications residing on the network. The NSA had the ability to order equipment to be taken off-line, rebooted, and could install filters and block ports.

- **Incident Response / Consequence Management Group (IR / CMG):**

The function of the six (6) individuals composing the IR / CMG was to respond to a significant network disruption or security incident using the organization's plans, policies, and procedures in order to contain, investigate, recover from, and report the incident or disruption. The City of Seattle, King County, and Washington State Department of Information Services (DIS) NOCs each had a six-member IR / CMG. The NOCs for the Washington State Department of Transportation (DOT) and Emergency Management Department (EMD) had a smaller group.

The activities of this group included, but were not limited to: analysis of the situation to determine potential consequences; employment of an organization's mitigative or defensive strategies and resources; documentation of the incident; forensic evidence collection; and investigation. The utility of the IR / CMG was similar to each participating organization's incident response team (IRT) or computer emergency response team.

Most IRT's have both an investigative and a problem-solving component. These functionalities resided in the NOC IR / CMG. This group included management personnel who understand the organization's security, emergency, legal, or network policies, and has the authority to act; technical personnel with the knowledge and expertise to diagnose and resolve problems; security personnel able to track security issues and perform in-stride and post-mortem analysis; or communications personnel able to keep the appropriate individuals and other organizations informed as to the status of the problem and, if necessary, assist in developing

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

crisis response strategies. One of the six members of this group acted as the leader for the organization's NOC.

- **Communications Operator**

The function of the communications operator was to monitor external communications (e-mail and telephone) for the NOC and relay information coming from these sources to the NOC.

EXERCISE CONTROL

An exercise Control Team oversaw the execution of this exercise and was composed of personnel familiar with the exercise objectives, process, and construct. This group monitored all activities throughout the exercise and adjusted the process as necessary to keep the participants oriented toward outcomes that support exercise objectives. The Control Team had overall responsibility for directing the exercise process, administration, and plenary sessions. Facilitators and data collectors appointed to each pod were members of this group. The Control Team also tracked and evaluated critical outcomes at the conclusion of each session. This group assessed the activity of each pod and, if necessary, provided supplemental information that clarified the scenario.

The exercise technical control staff resided with the Control Team. This staff generated scenario injects depicting the status of an organization's network for viewing on each pod's network status display and injected scenario elements depicting challenges that consequence managers would have to address.

The exercise Design Team indoctrinated members of the Control Team, stakeholder facilitators, NSAs, and communicators prior to the conduct of the exercise. Included in this training were:

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- The exercise process, including the organizational structure, the flow of activity, and the expectations at the end of each session. A walk-through of the participant handbook and facilitator guide also occurred.
- Exercise pre-play to demonstrate the expected levels of discussion and required session products.
- A tour of the exercise site to understand the flow of the interactive process and to prepare the pods for exercise activity.
- An indoctrination and practice period using the simulated network (NETSIM) display console and communication laptops.

This training provided members of this team with the requisite information and practice to effectively perform their roles.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

SECTION SEVEN

GAME PLAY

In addition to responding to the stimuli provided by the simulated network (NETSIM) and other injects, we tasked participants to prepare responses to questions addressing key issues associated with the theme of each vignette. During the plenary sessions held at the conclusion of each vignette, a member of each pod discussed the organization's responses to these questions. The following summarizes this activity and the players' discussions.

VIGNETTE ONE: NORMAL DAY AT THE OFFICE

The theme of this vignette was an “above normal” level of disruptions to the information networks of each organization. Using information and data provided through network status displays or injects provided by the Control Team, each pod responded to these stimuli by employing their incident plans, policies, and procedures. In addition to exercising these tools, during this session participants were tasked to review their incident response plan assumptions, review the internal and external communication flows of their Network Operations Centers (NOCs), and discuss relevant cyber-security issues. Following this, they identified and prioritized the organizational implications of prolonged periods of “above-normal” network disruptions and how these might influence planned processes, courses of action, and resource requirements detailed in their response plans.

Questions for Plenum

- **What does the Department of Homeland Security (DHS) “Condition Yellow” mean to your organization, in particular to its network security?**

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

City of Seattle:

- Practice information technology (IT) callout and alerting plan / verify numbers.
- Consider alternative work schedules of operational staff. If situation escalates, plan to maximize staffing & response capabilities.
- Increase frequency of review of firewall logs and monitoring of other intrusion detection systems.
- Pass advisory to department emergency contacts.
- Introduce measures outlined in BLUE advisory.
- Consider canceling or rearranging vacations and other time off to insure recall capability.
- Conduct security check on all critical systems.
- Be aware of physical access to restricted areas, e.g., communications closet, server room.
- Consider increasing frequency of backups, ensure offsite storage.
- Review network segmentation plans.
- Ensure employees (especially those with field / remote responsibilities) remain vigilant for spotting suspicious activities and behavior and are prepared to report it immediately to Seattle Police Department (SPD).

King County:

- Condition Yellow is normal (elevated level of network security post-Sept. 11).
- King County has developed an incident management plan detailing roles and responsibilities in the event of various disrupted services.

Washington State Department of Information Services (DIS):

- DHS Condition Yellow does not invoke any additional security activity at DIS. This situation is considered a normal activity.
- At Condition Yellow, DIS is at heightened awareness for physical issues -- such as building security.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

Washington State Department of Transportation (DOT):

- Send notification of increased alert level to employees for increased awareness.
- Increase frequency of system log scans.
- Contact response team members to coordinate a plan of action.

Washington State Emergency Management Department (EMD):

- Our organization is always at its highest level of network security.
- Block all executable files on a daily basis.
- Daily - run McAfee, updating DAT files.
- Daily - run IP Sentry to monitor network.
- Daily - run full back-up (13-14 hours).
- Subscribe to various LISTSERV - Multi-State (MS), SANS, Federal Computer Incident Response Center (FedCIRC).

• How is a “normal day” determined in your organization?

City of Seattle:

- Power is generated, water flows, bad guys get arrested, fires are extinguished, lives saved, people play in parks.
- National threat level is stable.
- Minor problems as indicated by number of Help Desk tickets.
- External pings – Internet Team notified of failures.
- Main systems up – no major outages.

King County:

- A "Normal Day" is assumed until indications are otherwise.
- An extraordinary day looks like:
 - Global outage.
 - Global e-mail server attack.
 - Global phone service disruption.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- Mainframe outage.

Washington State DIS:

- Monitor network on a regular basis.
- Experience on-going scans from the Internet.
- Develop and implement on-going security changes.
- Hold internal security meetings.
- Continue to monitor logging information.

Washington State DOT:

- Equipment failures, network configuration issues, training and use issues, SPAM, questions from customers about viruses, testing and application of system patches, responses to changing architecture software.
- More exciting than a normal day.
- System monitors indicate problems, notification of threats are received, and incoming messages are received that contain unknown content.

Washington State EMD:

- All network services are live and accessible.
- Network latencies to these services do not exceed 300 ms.
- Electrical services are functioning on commercial power.

- **What do you consider your organization's most significant cyber vulnerabilities?**

City of Seattle:

- Access levels to applications and data are not audited on a regular basis.
- Internal 802.11 Wireless and other remote access e.g., CDPD, Digital Subscriber Line (DSL), Inter-Governmental Network (IGN), Integrated Services Digital Network (ISDN).
- Employees: background checks, training, discovering wayward behavior.
- Gaps in communication protocols with other agencies / partners / vendors.
- Lack of policy and staff training for dealing with suspicious e-mails.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- Establish consequence management team (IT managers).
- Viruses externally introduced to the environment.
- Trust issues with sharing passwords and common logins.
- Lack of network segmentation and redundancy.
- Patch levels on old systems – legacy applications cause them to break.
- External virtual private network (VPN) Access – lack of audit ability for firewall and virus protection.

King County:

- Limited County-wide standard for patch and configuration-management.
- Budget constraints prohibit us from implementing inter-department security standards.
- Very limited internal firewalls -- perimeter security only.
- Some external-facing resources on internal network segments (available to public).

Issues:

- No inventory of structured query language (SQL) database and IIS servers within the County network.
- Policy guidance for investigative queries from legal entities.
- Governing authority by ordinance to set and enforce security policy (cyber world).

Washington State DIS:

- Non-disclosure agreement (NDA) would be required before we can answer this question.
- Standard e-mail and Web portal traffic, security awareness.
- In a confederation of government organizations, we are subject to the "weakest link" syndrome.

Washington State DOT:

- Lack of backup data "hot" site should the primary become unavailable.
- Incoming e-mail / viruses from attachments.
- Lack of monitoring tools.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- Social engineering.
- Constantly changing architecture of hardware and software.

Washington State EMD:

- Our biggest vulnerability at this point is our single connection to the Internet through DIS. We have redundancy.
- Lack of internal firewall / intrusion detection systems (IDS)
- Currently, only e-mail is authorized to be transmitted on the State Governmental Network (SGN). Authorization and setup of VPNs is time consuming and cannot be done solely by EMD.
- Internal customers storing files with viruses on their computers. Internal firewalls on each computer are needed and will be installed in the immediate future.

Solutions to overcome these challenges:

- Additional funding is being sought to install two new T1s for Internet connectivity. One T1 should be to a tier one service provider such as Sprint or Uunet. The second T1 should be satellite providing Internet connectivity. All of our circuits will be on physically diverse routes terminating in geographically diverse regions.
- We have purchased and will be installing firewall and IDS systems as well as routers specifically for doing our perimeter or outer layer of cyber-security.

What single events might cause your Incident Response Team (IRT) to activate?

- A local area network (LAN) outage causing disruption to more than 10% of the network services.
- A wide area network (WAN) outage.
- Detection of a virus / worm outbreak.

What cumulative events might cause your IRT to activate?

- Network probe accompanies by an intrusion or intrusion attempt

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

VIGNETTE TWO: COORDINATED ATTACKS

The theme of the second vignette was a low-level coordinated cyber-attack against stakeholder organizations. Players addressed issues or actions necessary to respond to these attacks in a combined manner and to resume network operations. After recognizing indications of abnormal events, participants analyzed the problem and responded to re-establish the operations of their networks. Working in their respective NOCs, participants initially assessed the situation, implemented their response plans, and determined what additional actions, coordination, and/or resources were necessary. As the situation presented may become greater than what was anticipated by each organization, it may have outstripped available internal resources. This session provided the opportunity for participants to discover the need to revise policies, procedures, resource allocation, and/or communication flows to account for vulnerabilities identified by this vignette that were not addressed by the organizations' plans.

Questions for Plenum

- **What does the DHS “Condition Orange” mean to your organization, in particular to its network security?**

City of Seattle:

- Pass alert on to department emergency contacts.
- Continue or introduce measures listed in YELLOW advisory.
- Via call-out lists, contact all essential personnel regarding their recall availability.
- Exercise test alert of all 24 x 7 on call staff between departments and coordinate schedules for critical staff across departments.
- Test communications: e-mail, 800 MHz radio, carrier pigeon.
- Suspend public tours of infrastructure.
- Increase staffing and backup for system monitoring.
- Change passwords and physical access codes.
- Verify availability of key vendors.

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

King County:

- Notify staff and review policies and procedures on how to respond to an attack that occurs during DHS Condition Orange. Condition Orange would command different actions from those previously executed in Condition Yellow.
- Communicate with other agencies to coordinate policies and procedures that are implemented at various DHS alert levels.

Washington State DIS:

- Increased security in all buildings.
- Broadcast message to all DIS personnel about heightened state.
- Be more vigilant, higher awareness among receptionists to ask for ID.
- Facilities staff would ensure backup generators, etc. are ready to go.
- Network Security: same as "usual day" activities, with reinforcement among staff to be aware of their surroundings and people in the area.
- Look for anomalies in network activity.

Washington State DOT:

- Limit physical access to computer facilities.
- Deny access to outside vendors.
- All non-DOT IT personnel will be escorted at all times.
- Increased attention to system monitoring.

Washington State EMD:

- How does this differ from a "normal level" of security? It does not.
- How does this differ from DHS "Condition Yellow"? It does not.
- **What is the role of your IT organization in the emergency management organization?**

City of Seattle:

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- Provide logistical and communications systems support,.
- Monitor IT infrastructure status
- Respond to IT related problems
- Restore service, e.g. radio, telephone, computer network, e-mail, messaging, file and print services, dispatch, and critical databases.

Gaps:

- Focus on City IT resources as an asset, implement policies and practices to safeguard, protect, facilitate recovery and assure continuity of business.

King County:

- Provide support to King County Emergency Organization.
- Clarify access procedures regarding King County "meet me" room locations.
- Clarify access procedures for Comcast POPs.
- Clarify physical access requirements for all staffing and networking areas relative to DHS conditions.

Washington State DIS:

- DIS has a practice of sharing security incident information with EMD through the Washington State Computer Incident Response Center (WACIRC)
- DIS general rule is to:
 - Be a focal point for sharing security information with regional partners.
 - To conduct incident notification and response coordination.
 - To carry out monitoring and mitigation for SGN and IGN systems, and regional partners (City of Seattle, King County EMD, and DOT).
- DIS Computer Incident Response Team (DISCIRT) was formed in 2002 as an IT organization internal to DIS. DISCIRT is the starting point for statewide incident response that includes EMD.
- DIS and EMD have joined the multi-state Information Sharing and Analysis Center (ISAC) started in New York. EMD represents the physical side, DIS represents the cyber side.

Washington State DOT:

- External - communication with WACIRC via e-mail, fax, pager, phone, and cell.

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

- Internal - As a support organization for our internal Emergency Operations Center (EOC). We specifically support EOC e-mail and hardware (printers, PCs, faxes, etc.).

Washington State EMD:

- To help coordinate resources when the resources of the local jurisdictions are overwhelmed. To act as liaison between the Local, State, and Federal response agencies.
- **What are your recommendations for a regional response / defense to a wide-scale cyber-attack?**

City of Seattle:

- Develop relationships and protocols related to vertical lines of business: public safety, utilities, human services, etc.
- Organize an inter-agency “Crisis Response” Team to immediately activate and begin analysis and classification of the agent of attack and coordinate response in a real time manner.
- Support LISTSERV for WACIRC Level 2 & 3 problems.
- Activate and communicate with WACIRC, once activated by DIS for Level 1 problem.

King County:

- Establishment of inter-agency communication points of contact list.
- Create inter-agency roles and responsibilities plan.
- Analyze data generated from a host-based and network-based IDS inside King County Wide Area Network (KCWAN) perimeter.

Washington State DIS:

- Early information sharing about potential security incidents and status of incidents in process.
- Central coordination through regional and statewide LISTSERVs. Out-of-band, non-dependent notification system is in place for WACIRC. All regional partners should consider similar.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- Process for states, cities, and counties escalating to federal and international agencies is not yet solidified.

T2 AAR #041

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

Washington State DOT:

- Obtain management approval for dropping outside internet connectivity.
- Increase system monitoring effort.
- Increased reliance on out-of-band communications.
- Have Public information Officer (PIO) send alerts via television stations carrying DOT camera feeds.

Washington State EMD:

- In this case, the best defense is a good offense. Having cyber-security best practices in place.
 - Having redundant paths to your services.
 - Early detection determination, and warning with IDS and firewall protection.
 - Coordinating response efforts with stakeholders and vendors involved.
- **What is your organization's responsibility to entities outside your jurisdiction with regard to a wide-scale cyber-attack?**

City of Seattle:

- Post WACIRC Level 2 and 3 incidents to LISTSERV.
- Contact DIS Help Desk for Level 1 incidents.
- Contact King County operations and management.
- Engage Internet Service Providers (ISPs) in incident response.

Gaps requiring clarification:

- To be determined (TBD): relationship with FedCIRC, National Infrastructure Protection Center (NIPC), DHS.
- Suburban cities: utility services.
- Business Partners: regional wholesale water and power customers.
- Regulatory Bodies: Environmental Protection Agency (EPA), Department of Energy (DOE), Federal Energy Regulatory Commission (FERC), North American Electric Reliability Council (NERC), Western Electricity Coordinating Council (WECC).
- Auditors.

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

King County:

- Notification and coordination.
- Mitigation of attack traffic.
- Information sharing relative to temporary or permanent solution.

Issues:

- King County needs a policy for inventory of externally facing websites and where they logically reside within our King County network. This will allow us to better mitigate risk.
- King County needs a global security policy relative to DHS conditions.
- Review authorities for threat conditions.
- Cooperation / coordination with Canada.

Washington State DIS:

- Federal:
 - Provide for information on suspected illegal activity.
 - Communication and notification about incidents that could have national impact or that could be coming from other nations.
- City/County:
 - Primary responsibility is notification.
 - Cities and counties who have computing assets in DIS environments.
- Neighboring states:
 - Currently, no process for providing information. Responsibility as good Net citizens is to notify them that there may be a threat against them.
- Canada:
 - Currently, no process for providing information. Responsibility as good Net citizens is to notify them that there may be a threat against them.
- Example in exercise - requested specific network information from British Columbia (BC) to allow us to block the worm coming from the SGN directed toward them. We also notified them that we had blocked traffic.

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

Washington State DOT:

- Develop information exchange with DIS / WACIRC to coordinate response efforts.
- Notify Public of any impact to any DOT external web sites, traffic cameras, ferry schedules, etc., via PIO release.
- Being a good neighbor and alerting others in "neighborhood."

Washington State EMD:

- Our procedure is to notify our local emergency management facilities of the threat and have them contact DIS for further information regarding the IGN or SGN.

T2 AAR #041

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

VIGNETTE THREE: WMD FORCE MULTIPLIER

The theme of the final vignette was an overwhelming, coordinated cyber-attack acting as a “force multiplier” for a combined terrorist WMD attack. Issues and actions necessary to re-establish or maintain network operations to permit crisis and consequence management were addressed by the NOCs. In a process similar to the previous sessions, participants received indications of the events leading to significant disruptions to critical networks. Participants then assessed the situation and took necessary actions to re-establish these networks to enable necessary response and governmental operations to continue.

Questions for Plenum

- **What does the DHS “Condition Red” mean to your organization, in particular to its network security?**

City of Seattle:

- Assumes Orange readiness in place, plus...
- Stop all IT changes.
- Mayor declares emergency, activates EOC.
- Take specified actions geared to whether Seattle assessed as a target.
- Deploy a 24x7 NOC.
- IT infrastructure staff scheduled 24x7 for EOC.
- Confirm call-out information and notify all IT staff.
- Notify all IT customers of potential emergency disruption of services.

King County:

- Obtain intelligence.
- Obtain direction from King County High Level Officials.
- Establish POA consistent with King County plans and Policies.
- Posture and respond accordingly.

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

Washington State DIS:

- Increased security in all buildings.
- Broadcast message to all DIS personnel about heightened state.
- Be extremely vigilant, higher awareness among receptionists to ask for ID.
- Facilities staff should ensure backup generators, etc. are ready to go.
- Network staff would be on heightened awareness, with reinforcement among staff to be aware of their surroundings and people in the area, watch more closely for anomalies in network activity.
- Review logs more carefully and backup systems more frequently.

Washington State DOT:

- Notify all employees of change in threat level.
- Ensure 24-hour access to management team regarding threat level.
- Poll and brief IT emergency response personnel.
- Continuous monitoring for IT infrastructure abnormalities.
- Increase physical security at IT facilities (possible assistance from Law Enforcement / National Guard).
- Ensure operational condition of backup power generators.

Washington State EMD:

- Awareness and monitoring.
 - How does this differ from a "normal level" of network security? No difference.
 - How does this differ from DHS "Condition Orange"? No difference.
 - What extraordinary actions do / might you take under this threat condition? Increase physical security to our network hardware.
- **If a regional NOC undergoes a “catastrophic” loss, what resources might your organization offer to support the NOC’s continuity of operations?**

City of Seattle:

- Staff.
- Vendor relationships.

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

- On-call expertise.
- Diagnostic support.
- Communications support.
- Provide alternative sites for hosting of critical Public Info Web pages and Critical Response and Recovery Applications.

King County:

- Physical location.
- Workstations.
- Network accessibility.
- Personnel.
- Voice communications capabilities.

Washington State DIS:

- DIS could act as a conduit to provide possible network technical staff assistance.
- Possibly provide hardware / software network assistance and a facility (management decision).
- Leverage vendors to get priority delivery for equipment and services, and public information assistance.

Washington State DOT:

- Use of satellite-based internet connection
- Use of 800 MHz radio system

Washington State EMD:

- Talking to vendors and making sure that TWP is being followed.
- **If this loss occurred to your organization what resources might you need and how would you get them?**
 - Satellite Internet connectivity. Purchase dish from a local vendor and activate service.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- **What are your major requirements for a “NOC in a box”?**
 - 24-hour switch, liquid crystal display (LCD) / keyboard, video, mouse (KVM) switch, 1 dual=processor Win2K=based server not to exceed 4U.
- **If your organization’s networks are degrading gracefully, but rapidly, what are your priorities for system continuity?**

City of Seattle:

- Systems and Infrastructure required to manage IT resources.
- Ports, segments and servers required for Public information and internal coordination of event--e.g., e-mail.
- Utilities: distribute water, provide drainage distribute power, generate /buy / sell power, serve critical customers, bill customers (Supervisory Control and Data Acquisition (SCADA), wholesale B2B links, Out-dialer, Interactive Voice Response (IVR), On-call, geographical information system (GIS) / Asset Management., etc.).
- Public Safety: 800 MHz radio, dispatch, mobile communications, records systems.
- Administration: post payments, pay employees, make purchases, pay vendors.

King County:

- Protect critical applications.
- Communicating with systems and application owners to ensure they implement their business continuity plan.
- Investigate the cause and develop a protection plan.
- Inform the public of the impact.

Issues:

- Policies and procedures do not provide a process to formulate response (e.g., assess, define challenges, and develop response options).
- How to coordinate internal activities?
- How to coordinate external activities?
- Intelligence behind the decision to escalate to Condition Red -- what does it mean to us?

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

T2 AAR #041

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

Washington State DIS:

- Keep Access Washington running for the Governor and other government organizations to use as a communication tool to the public - in support of public safety, health, and welfare.
- Work with customer agencies to prioritize and keep network resources up that support emergency services.

Washington State DOT:

- E-mail and phone systems are the most critical support assets for Transportation infrastructure recovery.
- Public internet access can be jettisoned as a means of maintaining internal system integrity (PIO can be employed to establish and maintain public information flow).

Washington State EMD:

- Network hardware (routers, switches, firewalls, IDS, VPN).
- Servers (Domain controllers, Exchange, Dynamic Host Configuration Protocol (DHCP)).
- EOC Workstations (Based on needed pods).
- Printers.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

EVACUATION PHASE -- KING COUNTY RESPONSE

As a result of the scenario induced effects, King County was forced to evacuate its downtown facilities with no opportunity to perform maintenance and critical system configuration changes. All employees in the downtown areas evacuated, with critical management personnel assembling to assess the initial consequences and define a course of action to restore services to the employees and the public. Management chose to perform the following:

- Define the situation.
- Identify the major challenges.
- Identify solutions.
- Summarize the impact sustained by this crisis.

The following products were developed:

- **Problems encountered by the crisis**

- The following facilities were evacuated:
 - Jail
 - County Courthouse
 - All of King Street
 - Key Towers
 - Wells Fargo
 - Exchange
 - Etc.
- All Core cyber-services abandoned and in an immediate state of decay.
 - Transportation system was affected.
 - Impacts on employees evacuated.
 - Work status is undefined, organization is in disarray.
 - Accounting functions are lost and driven to manual recovery and restoration.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- **Challenges facing King County**

- Safety of staff.
- Restoration of essential services poses challenges in the following areas:
- Restoration of security and infrastructure.
- PIO (information to employees and public) / critical function restoration / confidence building actions to restore public confidence.
- Legal challenges and authorities - who will make decisions during the rebuilding process - especially early when many employees are without a workplace?
- Coordination and Leadership with respect to restoration activities.
- Prioritization of required actions and activities.
- Human Resources.

- **Solutions**

- Evaluate and assess facilities and capabilities.
- Contract / define alternative facilities - some are defined in plans (work through Property Management).
- Establish initial network connectivity (including home connections).
- Develop work plans and assignments.
- Develop plans to communicate to internal and external audiences.
- Organize internal and external agencies.
- Coordinate with other agencies.

- **Impact of the Crisis / Evacuation**

- In a week
 - Few lost or essential services will be restored. System is in a state of decay.
 - 911 will have been rerouted.
 - Buses are running.
 - Sewage treatment is operating.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- Payroll is questionable - a stop-gap manual method at best will be in operation.
- Human resources will be strapped.
- Court system is not operational.
- Public safety and confidence in disarray.
- In a month
 - No significant improvement in the Data Processing System.
 - Limited improvement in the other systems.
 - Automatic funds transfer payroll is still a problem - in manual mode.

It was assessed the County services would take four to six (4-6) months to be fully restored.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

TOPOFFs QUESTIONS DURING VIGNETTE THREE

- **What does DHS “Condition Red” mean to your collective organizations?**
 - How might you coordinate your cyber-security operations in this threat condition?
- **What are the most critical elements of your IT infrastructure?**
 - If your organization’s networks are degrading gracefully, but rapidly, what are your priorities for system continuity and restoration?
- **In the event of a wide-scale cyber-attack that disrupts significant portions of your critical infrastructure, from a cyber perspective, what are the essential elements of information that TOPOFFs need?**
 - How do you get this information?
- **How do you regain and maintain public confidence that government organizations can respond and provide for adequate security to critical infrastructures, particularly the IT infrastructure?**

The major findings for the top officials are as follows:

- There are corollaries between a physical attack and cyber-attacks as to the impact on the continuity of operations of governments and their agencies. The ability to react to a physical attack or natural disaster has appropriate processes in place with the role of the Federal government understood by the State and Local governments, this is not true when there is a cyber-attack.
- The ability to maintain IT infrastructure is predicated on the fact that individuals will be able to get to their workspace. In those instances where this is not true, the impact on the IT infrastructure of the various government agencies varied as to their ability to do backups and to access their systems from alternate locations.
- During the pre-exercise period, the Federal government was changing its official way of responding to cyber-attacks through the standing up of DHS and its assimilation of a number of organizations with cyber-responsibilities. The attempt by the Federal government is to develop an integrated cyber-response capable of many tasks to include support

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

to both State and Local governments. There is still a need for a single point of contact within the Federal government for the dissemination of information related to cyber-attacks to the State and Local governments.

During Vignette 3, TOPOFFs received a phone call from the Office of the Secretary of DHS. In the phone call, he asked participants to provide an update to him on the status of the situation and any assistance they may need. The following is their response:

THIS IS AN EXERCISE

This is in reply to your faxed questions of DTG xxxx May 7, 2003. (TOPOFF2 Exercise Messages)

1. We are experiencing several denial of service interruptions over several of our networks most are tapering off, many Websites have been defaced and Hackers have attempted to add additional confusion and delay first responder actions through a misinformation campaign over official government sites. King County NOC a key information node has been evacuated and is in the process of determining how to restore services since no backup facility exists.
2. While the cyber-attack has not affected 1st Responder's ability to attend to the WMD incident, there has been disruption of our ability to respond to other effected populations; but on a limited basis, we are working through these issues. Our concern is what information being broadcasted to the general public through media outlets.
3. We have our FEMA LNO at the State EOC, and have sent our LNO to the DOJ JOC, DOE FERMAL assistance is inbound for plume definition and advise local medical responders to treat contamination individuals. FBI is conducting an investigation into the attacks. Alternate communications were established with NCS using SHARES.
4. We need you to provide resources to assist in the rapid restoration of the jurisdictions networks. A unique, single, federal response cell is needed to assist in the coordination of restoration of our communication and information networks.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

HOT WASH-UP

The Hot Wash-up concludes the interactive portion of this exercise. Each group presents the significant and unresolved planning and management concerns, critical issues, and recommendations identified in each session. As part of this activity a moderated discussion among participants will occur. The outcomes of this plenary session requiring action will be carried forward by respective organizations and will be included in the final report.

- **What are the three most significant insights gained from TOPOFF2 CYBEREX?**

City of Seattle:

- Need a clear prioritization of services, assets, and functions for return to service (business continuity).
- Need a co-located IT management level consequence team for “real.”
- Need a working definition of “normal” and thresholds for triggering escalation.
- Ongoing “tug of war” between adding and sustaining services vs. security vs. cost.
- The high-level view of system status is important.

King County:

- Need a review of Policies and Procedures to better reflect activities required under DHS Alert Conditions.
- Must define authorities consistent with Alert Conditions and span of control among King County agencies (Who has precedent?).
- Transfer of authority (How does it occur? How do we identify the need?)

Washington State DIS:

- We affirmed that our incident response plans and processes are effective.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- Communications capabilities, having them and using them, are a key to success.
- Learning how other organizations work in similar situations, and where gaps are in response integration across jurisdictions.

Washington State DOT:

- The complexity of regional IT structures in the Pacific Northwest.
- A greater appreciation for "normal day" services from many different government providers.
- The inter-relationships of all governments providing IT support for public health and safety, and significance of (and risk to) the Washington State DOT DMZ services.

Washington State EMD:

- Coordination between Local, State, and Federal entities is critical.
- Redundancies in systems and networks are needed, to include "Hot" or "Warm" sites.
- Normal security measures need to be at their highest level.

- **What are the three most important recommendations we intend to take home?**

City of Seattle:

- Bring Incident Command System (ICS) to cyber-response: NOC, Management CIRT team.
- Need the system-wide network management view / map complete with a network segmentation plan.
- Need web site redundancy, backup, and redirection.
- Need a redundant NOC.

King County:

- Review Plans and Procedures to reflect observations from this exercise.

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

- Develop procedures for an integrated cyber and physical approach to security (remembering that there is a physical element to cyber protection).
- Develop procedures for physical relocation and restoration of services.

Washington State DIS:

- Develop backup or alternate methods for obtaining information when primary resources are compromised.
- We want to work on solidifying our regional notification and response strategy for cyber events.
- We want to review our own processes for upper management notification and issue escalation during incidents.

Washington State DOT:

- Continue established relationships and maintain current contact information, especially fax numbers.
- Define regional IT standard actions for each threat condition (THREATCON) level, publish guidance and keep current.
- Share RIIG information with Washington State DOT directly.

Washington State EMD:

- Revisit restoration plans and priorities, both TSP and internally.
- Refine plans for IT COG with government and industry.
- Assist in all efforts to improve the coordination between the IT and Emergency Management communities at all levels, industry, Local, State, and Federal.

- **What is the most significant operational cyber-security question that we still need an answer to?**

City of Seattle:

- What is our dependency on external cyber-nodes?

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

- Where is the money coming from?

King County:

- How do we elevate the priority of cyber-security at levels above operations to defend against the growing threat?

Washington State DIS:

- How, when, what.... gets conveyed to the Federal level during such incidents? And to whom?

Washington State DOT:

- What is clear-cut definite authority needed in an emergency to decide when to do the following:
- Employ internet filters, block external ports.
- Take down external servers.
- Hardening of internal devices and isolating internal routers.
- How do we prioritize services / systems capabilities in a changing emergency environment?
- Is there a basic protocol?
- Will "best judgment" guidance be used?

Washington State EMD:

- Improving, improving, improving... Takes everyone sharing information.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

State of Washington Department of Information Services

TOPOFF2 CYBEREX Review and Assessment

Introduction

On May 6-7, 2003 the Washington Department of Information Services (DIS) participated in the TOPOFF2 Cyber Exercise (T2 CYBEREX) at Camp Murray. Funded by the National Institute of Justice and designed and executed by Dartmouth's Institute for Security Technology Studies (ISTS), the T2 CYBEREX was conceived to test local, state, and federal response capabilities in the event of a coordinated physical and cyber-attack. While the CYBEREX was conducted separate from the federal TOPOFF2 initiative, it referenced the same physical event as the main exercise – using the cyber-attack as a force multiplier.

Participants in the T2 CYBEREX included DIS, the City of Seattle, King County, Washington Department of Transportation, and the Washington Emergency Management Department. Support resources from commercial and federal entities were also included in the exercise.

The primary focus of the T2 CYBEREX was to test, “The ability to respond to the challenges posed by anticipated and unanticipated disruptions of government-related information networks due to a large-scale cyber-attack within the framework of a WMD event will address the requirement for increasing complexity.” According to documents prepared by the exercise developers, the exercise scenarios were focused on helping the participants evaluate the following:

- The effectiveness of the various cyber-security plans, policies and procedures of the City, County, State, and Federal levels to adequately address issues and support the response for a large-scale cyber-attack on government-related information networks.
- The ability of participating network operations centers to organizationally integrate and effectively conduct or manage a sustained response to a cyber-attack.
- The planned flow of communications and information in an operational context.
- The decision and coordination processes in a range of potential consequences.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

The specific objective of the Department of Information Services was to “Determine that WACIRC procedures - including incident reporting, response, escalation, communications, containment, etc. -are sufficient to effectively mitigate the effects of cyber-attacks.”

Issues/Observations

Because the exercise involved the use of a simulated network environment, simulated support services, and narrowly controlled communications vehicles (single terminal for all email, listserv, and telephone communications), the primary focus of the DIS Team evaluation was on the following:

- How decisions were made
- Clear and measurable escalation policies
- How do we interact internally (DIS Incident Response Team to DIS Management)?
[Internal Interaction]
- How do we interact externally (DIS to state agencies and regional partners)?
[External Interaction]
- Use of available resources

An overall assessment of the performance of the policies and practices of the DIS Computer Security Incident Response Team (DIS CSIRT) and the related Washington Computer Incident Response Center (WACIRC) processes indicates that the significant work done in developing and implementing these programs has paid great dividends. The DIS CSIRT team worked effectively in developing and implementing response activities as well as coordinating effective communications to impacted parties. This was clearly a result of sound and tested processes combined with quality, well-trained personnel.

While no key processes were absent, DIS understands that the key to an effective incident response process is to engage in continuous process improvement. To that end, the DIS team used the T2 CYBEREX to identify areas that would benefit from further assessment and process improvement activities.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

The identified issues/observations include:

1. Improved categorization of incident severity levels

- Define distinct communication processes for all DIS CSIRT Severity Levels (SL1, SL2, SL3).
- Determine criteria for declaring SL1 when multiple agencies are effected.
- Define metrics for declaring SL1/SL2/SL3 and security incident.
- Determine if there is benefit in mapping the DIS CSIRT Severity Levels more closely with the color-coded federal kinetic alert indicator model to enable better communication on a federal level.
- Investigate feasibility of using the multi-state ISAC cyber-alert indicator model, which maps to the federal kinetic alert indicator model.

2. Improved management communication and engagement

- Refine the processes by which high priority security incidents are elevated to DIS management, specifically to address:
 - Specific procedures for communication with DIS Management, DIS Director, and the Governor's office, during a security incident.
 - The process and criteria for notifying DIS management of specific impact to DIS services.
- Establish a DIS CSIRT “management” liaison for communication with DIS Executive Management during a security incident.

3. Improved customer communications

- Review process for notifying customers of impact to DIS services (WA-STATE-NOTIFICATION listserv). Include marketing the listserv, and security process training.
- Review and adjust the current hacked web site process to include determination of whether DIS hosts the compromised customer agency site or the customer hosts the compromised site and the communication process for both DIS-hosted and customer-hosted sites.

4. Improved regional communications

- Define the process for communicating to PIOs @ City of Seattle and King County during a security incident.
- Pursue the use of the Regional Incident Intelligence Gathering (RIIG) listserv with regional partners.

5. Improved “public” communication

- Define what information is released when a state web site has been defaced.
- Define WACIRC/DIS CSIRT roles in disseminating information when non-network, non-state related major event occurs (RDD, 9-11, threat level RED).

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

6. Improved use of external resources

- Obtain "preferred" status (sign up for alerts/early warning) for DIS with CERT.
- Who/How/When to notify "Feds" or in getting information, or securing any additional resources.
- Develop "back up" or alternative methods for obtaining and validating information when primary resources are compromised (i.e., commercial web sites, Internet access, private security resources, telephones, etc.).

7. Improved response procedures

- Review and document process and procedures to quarantine a potentially compromised device (Who? How? What procedure and under what authority) WACIRC recently adopted "WACIRC Law Enforcement Guidelines for Reporting and Responding to Computer Crimes.
- Revise web page defacement incident response procedure to include check for DIS hosting.
- Document the procedure for notifying DIS IT when Access WA link must be removed or restored.
- Obtain Law Enforcement notification process and procedures for state agency web page defacement. (See WACIRC Law Enforcement Guidelines for Reporting and Responding to Computer Crimes).
- Add full set of all DIS contact numbers to Incident Response Handbooks.
- Define the process, procedure, and actions taken for the DIS CSIRTeam and cyber incident response, should the US move to "threat level" RED.
- Review DIS Disaster Recovery Plan for node sites impacts and communications during "physical" events.
- Define DIS CSIRT involvement in combined Cyber/Physical incidents.
- Develop process and procedure for responding to a security incident of exceptional long duration. (i.e. 24 hour staffing, staff relief or rotation, home/family staff needs, site evacuations, etc.).

Resulting Actions

Under the direction of the DIS CSIRT Coordinating Team, actions are already under way to address the issues identified during the T2 CYBEREX. The following is a summary of some of the current activities:

- A DIS CSIRT Severity Level Evaluation Subcommittee has been formed to address incident severity categorization issues
- DIS Communications personnel assigned to the DIS CSIRT team have initiated the develop and documentation of updated communications procedures and will provide appropriate training to DIS CSIRT personnel

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- All of the identified issues have been assigned to a recommended lead resource(s) and oversight of the issues has become a regular part of the DIS CSIRT management process.
- A draft “Rules of Operation” for the proposed Regional Incident Intelligence Gathering (RIIG) Listserv has been prepared. Planning is underway to engage the regional T2 CYBEREX participants in finalizing the “Rules of Operation” and initiating a pilot operation of the RIIG listserv.

Conclusion

It is the collective opinion of the those DIS personnel who were involved in the T2 CYBEREX that the investment of time and resources in exercise participation resulted in significant value in both the confirmation and potential improvement of incident response communications processes and the benefit of expanding the boundaries outside of state government to city and county government organizations as well as our private industry partners. The DIS CSIRT team and WACIRC participants look forward to addressing these issues in a continuous effort to provide the best possible environment to protect the information assets of the State of Washington.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

King County Perspective of TOPOFF2 Cyberex.

Purpose

This document is King County's preliminary after-action-report (AAR) for the exercise. The point of contact for comments and updates to this report is (b)(6) in the Information and Telecommunications Services Division of the Department of Executive Services.

Exercise Participants

The Top Officials 2 Cyber-Terrorism Exercise (TOPOFF2 CYBEREX) was conducted at the Washington State Emergency Operations Center on May 6-7 2003. An orientation session for some of the key participants was held on May 5th. TOPOFF2 CYBEREX was designed and controlled by the Institute for Security Technology Studies (ISTS) of Dartmouth College. Primary exercise participants included the City of Seattle, King County (DES (ITS), KCSO, DNRP, DoT (Transit)), and the State of Washington Department of Information Services (DIS), Emergency Management (EMD) and Transportation (DOT). In addition, a group of senior managers from each public agency served in the role of "Top Officials." For King County, this included DES (ITS and OEM), KCSO, and PAO. Representatives from the University of Washington, Microsoft, Boeing, Qwest, the U.S. Secret Service (representing the Seattle Joint Task Anti-Terrorism Task Force - FBI, USSS, US Attorney's Office), and the National Communications Systems (representing the Department of Homeland Security) were present, serving as a support pod during the exercise.

Exercise Overview

The exercise occurred in three scenarios or vignettes: (1) normal day at the office, with "normal" network and computer problems; (2) an escalating series of events - computer

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

and network problems which might be preliminary symptoms of a directed cyber-attack; and (3) a major cyber-attack on participants' computer networks, coupled with a weapons of mass destruct (WMD) attack – a radioactive detonation device (RDD) terrorist bomb exploding in Seattle.

Exercise Play

The CYBEREX was computer-assisted. Each participant group or “pod”, the controller functions and the support pod had computer terminals to use for communication with each other. In this fashion the communications between functions (communications normally conducted via telephone, fax, pager and e-mail) were captured for later analysis. In addition, ISTS developed a simulated network for each agency. This network was represented on a network map displayed on computer terminals, and included functions such as end-user computers, network switches, firewalls, e-mail servers, application servers (applications such as computer-aided dispatch systems or world-wide-web sites), and the networks linking such devices and linking agencies with each other and with the Internet. A series of injects occurred during the exercise. These events included, for example, failure of network switches or applications, failure of electronic mail, overloading of devices or firewalls by a flood of traffic (a “denial of service” attack), defacing or “hijacking” an agency’s website – placing false information on the site to incite public panic; and physical evacuation of key buildings. But the CYBEREX play was mainly about team working relationships. In response to each event, the participants’ teams – both technical teams and management teams – had to determine and implement a technical response to the event, and a management or top officials’ response to the event.

Injects (For reasons of confidentiality, this is not a complete list)

- Computer virus attack.
- “Worm” propagated via the Internet (A “worm” is a malicious computer program which exploits a specific vulnerability in commercially available software. Worms usually have payloads intended to cripple computer systems or networks.).
- Defacing or “hijacking” a government web site (intent: provide misinformation to the public).

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

- Cyber-attack on government computer systems coincident with a physical or kinetic attack, e.g. weapon of mass destruction.
- Attack by rogue computer programmer or team intended to breach, commandeer or compromise a key governmental computer system or network.

Vulnerabilities (For reasons of confidentiality, specific vulnerabilities are not listed here.)

What Worked

- An ad-hoc IT management team assembled specifically for this event made key decisions which prevented compromise of some key systems and networks, reducing the effect of the attacks on the simulated county government network.
- We have a large amount of redundancy in our existing IT infrastructure which is quite useful when the primary systems fail or are attacked.
- Collaboration with the City of Seattle and Washington State agencies proved very valuable. The preliminary workshops leading up to the CYBEREX were of good value and well attended. The ability to identify peers with similar interest.

Lessons Learned

- The County's siloed culture is a strong inhibitor to an effective inter-agency response. A major cyber-incident or even our response to a major natural disaster is likely to require a coordinated effort, at least for the departments with major IT resources and dependencies. If we daily work in a siloed environment, that is the way we are likely to respond in a major disaster.
- The cyber-environment is becoming more difficult to assess. We do not completely understand a "normal" day. Normal days are filled with many small cyber-incidents, computer and network problems which may or may not be indicative of looming larger issues. Related to this is our need to promote more peer to peer exchanges of information to help with the early detection of a potential major incident.
- Physical co-location of the team during a cyber-event vastly speeds decision-making and actions to counteract attacks. The Network Operations Center (NOC) we simulated for the CYBEREX is analogous to the EOC activated during disasters. While we have facilities at the Key Tower that could support inter-agency NOC activities during a major incident, we have no fall-back facility if we lost the Key Tower.
- Having an integrated team (staff responding to actual cyber-incident as well as staff supporting IT management response) was not effective. It was too easy to focus on the details of some of the technical issues and miss management issues that also needed attention.
- No participating government agency (and perhaps few or no private firms) fully understand our dependence on external cyber-nodes – places where private telecommunications networks meet and interconnect.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

Recommendations

- The County needs to more formally prioritize its business functions and, then, the related information technology services, assets and functions for return to service during disasters in general and cyber-attacks in particular (in order to maintain continuity of government and public confidence in government).
- The County should create a formal inter-agency incident response team that includes representatives who have real skin in the game. Having every County agency involved will not be effective. It is recommended that we explore a bifurcated structure with a group responsible for responding to the technology related aspects of the incident and another group responsible for supporting the management decisions and interagency communications. The efforts of the two should be closely coordinated with the former receiving direction from the latter.
- Existing response plans (e.g. ITS' Cyber Incident Response Plan, OEM's Homeland Security Plan) need broader distribution and vetting.
- Network segmentation plans – plans to purposefully break apart the County's internal network to protect key systems and functions – need to be more formal and more practiced.
- Interactive, computer-based, network views or maps, if created and maintained, greatly improve understanding of an event and our ability to react to it, in the same way GIS (geographical information system) maps are useful in understanding and responding to any disaster.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

City of Seattle Perspective of TOPOFF2 Cyberex.

What Worked?

- The established City of Seattle technical incident response team (called the Internet Infrastructure Team (IIT)) worked well together using established procedures to counteract many of the injects or events.
- An ad-hoc IT management team assembled specifically for this event made key decisions which prevented compromise of some key systems and networks, reducing the effect of the attacks on the simulated City government network.
- We have a large amount of redundancy (alternative paths or systems) in our existing IT networks which are quite useful when the primary systems fail or are attacked.

Lessons Learned

- We do not completely understand a “normal” day. Normal days are filled with many small cyber-incidents, computer and network problems, which may or may not be indicative of looming larger issues.
- Physical co-location of the team during a cyber-event (preferably in a City government NOC) vastly speeds decision-making and actions to counteract attacks. This NOC is analogous to the EOC activated by large public agencies during disasters.
- ICS can be formally applied to information technology (IT) teams responding to cyber-attacks.
- No participating government agency (and perhaps few or no private firms) fully understands our dependence on external cyber-nodes, those places where private telecommunications networks meet and interconnect.

Recommendations

- The City needs to more formally prioritize its business functions and, then, the related information technology services, assets and functions for return to service during disasters in general and cyber-attacks in particular (in order to maintain continuity of government and public confidence in government).
- The ad-hoc IT management team should be formally established and trained to make decisions during cyber-events.
- Interactive, computer-based, network views or maps, if created and maintained, greatly improve understanding of an event and our ability to react to it, in the same way GIS maps are useful in understanding and responding to any disaster.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

SECTION EIGHT

OBSERVATIONS

The following comments are based on player observations during the TOPOFF 2 CYBEREX.

NETWORK FORENSICS

In analysis of the "problems" witnessed, players relied heavily on normal diagnostic equipment that showed only aggregate (i.e. combined in & out) traffic rates, and simple indicators (e.g., green / yellow / red / black) about server status. This is typical of network management software, so this in and of itself is not a negative thing. During an actual attack, however, this does not provide enough information to allow a rapid response and reaction (part of their behavior may have been a side-effect of using the simulation, which is less detailed than the tools they are used to using).

In some cases, players asked more detailed questions from network provider support staff, but the standard modus operandi (MO) of typical regional network providers (and of the Northwest GigaPOP (Point of Presence) is not to do detailed traffic capture and analysis as a matter of normal policy and procedure to assist in incident response. This means that customers of large Internet Service Providers (ISPs) and GigaPOPs should have their own capability for network traffic capture and analysis. It is not known if this is typically something that GigaPOP customers know about and take into their own hands.

Further more, at the GigaPOP level, fine grained filtering on traffic based on classless inter-domain routing (CIDR) blocks or specific Internet Protocol (IP) addresses, or rate limiting of any type, is not a normally provided service. Bandwidth utilization is so great and the design of the network so optimized for speed and ease of management, that such services are simply not available or are not used in fear of affecting network availability or performance. Customers want to avoid blocking traffic using access control lists (ACLs) on their routers, to save router computer processing unit (CPU) cycles (and ingress interfaces on

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

a distributed denial of service (DDoS) victim's network are not the place to deal with a massive bandwidth consumption attack anyway). The upstream provider doesn't want to use ACLs on their routers, or rate limiting features, to save their router CPU cycles. Network operations will only provide all-or-nothing filters based on routing tables that leave customer networks either wide open or fully disconnected. This was the response that the Support cell gave to requests to block attack traffic to Canada in Scenario 2, and block Port 80 traffic in the face of a zero-day worm. (In the case of the first days of the Slammer worm, the Northwest GigaPOP did, for the first time, block all traffic to / from the affected user datagram protocol (UDP) port, but moved as quickly as possible to try to remove these filters).

Instrumentation in the network infrastructure that gives detailed information about traffic flows, in a form that can be easily provided to customers and shared in venues like Information Sharing and Analysis Centers (ISACs), and policies and procedures that supported network traffic capture and analysis, would greatly speed up incident response, especially in multi-site attack scenarios, such as Scenarios 2 and 3 in TOPOFF2. These services are not currently provided for many reasons, some of which are technical, some financial, and some political. As there is currently no significant demand for such services, or regulation requiring them, network providers are not voluntarily designing them into their networks.

HOST BASED FORENSICS

If one or more systems are found to actually be under attack (or involved as stepping stones in an attack) the contents of those systems' hard drives are critical evidence. During the exercise, the City team contacted Microsoft and the Computer Emergency Response Team (CERT) when an inject came confirming one of their systems was flooding a site in Canada. Microsoft requested the City provide the system to them to analyze, which the City agreed to. At that point, the City asked for assistance from the University of Washington (UW), but with the system physically in the possession of Microsoft, and no image copy of the drive made prior to handing it over to Microsoft, there was no way to independently

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

analyze the system (or to verify the integrity of the system) from that point on. Had this been an incident that involved law enforcement action, this could compromise an investigation. Had this been a real attack, the lack of initial recognition of the significance of the attack and the proper handling of potentially valuable evidence could have also delayed the response.

RESPONSE TO DENIAL OF SERVICE ATTACK

While handling the radiological dispersal device (RDD) force-multiplier attacks on web services of the City and State, players tended to not focus on the actual traffic going to / from affected servers, and in several cases their action was to ask for the systems to be taken out of service (which effectively accomplished a DoS as effective as the attackers were attempting). Given that they have little support to analyze traffic, and no option to rate limit traffic or block to / from specific IP addresses or CIDR blocks, there aren't many other options in the face of a concerted attack. This is a vulnerability that directly creates a situation where it will be impossible to guarantee 24x7 publicly available network based services (even though the general public may expect 100% availability).

Earlier, in the web server worm inject, players also used patching / rebooting and disabling of servers, to respond. The lack of detailed network traffic analysis capabilities (or perhaps just flow direction data in the simulation) made it so players could not accurately determine if their actions had in fact solved the problems or not. In one case, a player had asked for ports to be blocked by the network provider (whose reply that they would not honor that request was missed). Just after this, the attacker stopped the attack (which had the same effect of lowering the traffic line on the network graph), so the player thought the blocks had been put in place. When the attacker restarted the attack a short while later, the player (thinking the blocks *were* in place) could not tell if the worm had re-infected the server or if the server was attacking another site with outbound traffic. (A common theme was not asking "what traffic is flowing on my network and in which direction?" but instead asking "is the status green / yellow / red / black" and "how much traffic is flowing?") Without more detailed analysis tools and procedures in the simulation software, the players

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

found defense against a concerted attack extremely difficult. Again, this was an artifact of the exercise.

Responding to a DoS attack by blocking traffic based on black-listing specific IP addresses, ports, even blocking an entire protocol, can be easily defeated by shifting the attack methods. This means the most effective defenses against a bandwidth consumption or resource consumption attack will be rate limiting or white-listing to allow only a subset of known "good" traffic to get to a host / network. As was discussed earlier, however, these defenses are not available to the players from their upstream provider.

DOMAIN NAME SERVER (DNS) CACHE POISONING ATTACK

The DNS cache poisoning attack on the City of Seattle's servers redirecting them to a UW system could have had longer term effects because DNS time to live (TTL) values are set to long (in terms of response - typically 24 hours) values. Again, there would be little help provided in a normal situation from the Northwest GigaPOP (and perhaps not from commercial providers either, if the City uses any other providers.)

INFORMATION SHARING AND ANALYSIS

At the point in the exercise where teams knew they were attacked, there was no venue for them to disseminate information to other agencies above and below them regarding the attack. There is currently no state or regional ISAC, or other incident response related communication venue. All teams rely on the same network providers, but even at this level there is no means or policy for dissemination of information regarding an attack. Players had to ask the support cell if the same kind of traffic was being seen by other players. There was no regular status or warning service to push information out to, with the exception of CERT's standard advisories (even in the case of the Slammer worm, Washington State DIS, King County, the City of Seattle, and the Northwest GigaPOP did not voluntarily contact or share information among themselves. It was only when individuals took it upon themselves to make contact that communication in occurred). A new Research and Education Network

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

ISAC is now in place, but the Northwest GigaPOP and UW are currently not members of this ISAC.

T2 AAR #041

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

SECTION NINE

RECOMMENDATIONS FOR TOPOFF 3

- 1. Campaign-level cyber-attacks and attackers pay no attention to international borders.** These types of potential attacks are of most concern to members of the National Security Council and Homeland Security Council. The policy decisions related to attribution to a particular nation-state or equivalent adversary, and the practice of operational and strategic-level decision-making related to crisis coordination and consequence management between international stakeholders in government and private industry (including large multi-nationals) are critical areas that require further investigation and practice within an exercise environment. These will be examined a very basic level in Livewire; they are important enough issues to merit further advancement within TOPOFF.
- 2. Integrate physical attacks and consequence/crisis management with the consequences of the loss of critical information infrastructure.** Either engage operational managers of first responders in the cyber-exercise so that they could provide improved feedback as to the impact of the loss of critical IT services, or engage IT service providers in the physical side of the exercise.
- 3. TOPOFF 3 should be expanded to include multiple venues in the exercise.** Given the ability to distribute the exercise to many locations, we would suggest engaging multiple venues simultaneously.
- 4. The federal sector should be even more engaged.** Although the federal sector fully supported TOPOFF 2, we feel that due to the changing responsibilities in the cyber arena with the standup of DHS, it is important to include as many federal entities as possible in cyber play planned for TOPOFF 3. This would include the Department of Defense and possibly even include simulated attacks against the non-military networks of consequence management agencies such as FEMA, the CDC, and the private sector players such as the Red Cross.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

5. **Start early.** Exercises are new to IT departments. Police and fire have been doing them for years, but not IT departments. It takes a long time to bring them up to speed and explain what an exercise is, and what it is not. It is definitely not a vulnerability assessment, as many think. It takes time to build trust and understanding among the stakeholders. Each player needs to understand that the risk of failure is low, that they are not being graded or exposed to undue business risk, and that there is justifiable business value in improving their response capability through inter-organizational coordination and resource sharing. It also takes time to organize meaningful seminars.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

APPENDIX A

PROBLEM CHAINS

1. Background/Normal Activity:

These injects will be run-of-the-mill challenges that the network operators are accustomed to dealing with on a daily basis. There is no terrorist motivation for these injects, and they are largely unrelated to one another.

Equipment failures will affect all domains. Routers to city utilities and county metro transit will die. A router that connects state DOT to State DIS will die. A cable to the city PD will be cut. The email server at EMD will die.

Probing surges will periodically occur on all domains.

A wave of Spam will hit everyone.

Software vulnerabilities will be identified by CERT. Patches will be made available by Microsoft. The players can choose to be proactive or lazy in their response.

A Klez-like worm will spread an email message (spoofed from (b)(6) recommending lax security and containing insulting language.

2. The Super Flood (Code Red III) coincident with the WMD

This problem chain will be much like the Code Red worms in that it will exploit a vulnerability in a popular web server software application (IIS), scan for other vulnerable hosts, and then attack a series of government domains. It will also be a near zero-day exploit in that the vulnerability will be announced by CERT the day that the worm starts spreading (vignette2). Initial probes for vulnerable versions of the software on port 80 will be largely undetected in the normal volume of web traffic. Infected machines are both inside and outside of the stakeholder networks. The worm itself will be released in vignette 2, scanning for 15 minutes before going dormant. The malicious part of the worm will sleep for several hours before waking up to contact a master machine (overseas) for attack instructions. This could be done via a normal http get request. The master will provide the infected machines with a list of 50 IP addresses to attack which will be spread over the City, County, and State domains. The attack instructions will also specify how long to attack, and when to contact the master again for further instructions.

Several machines inside the City, County, and State will be infected, so that the attacks will be coming from both inside and outside. We may reward aggressive patchers by minimizing the internal infections in domains that aggressively patched after the CERT warning.

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

The attack mode will be modeled loosely after the Trinoo network of DDOS zombies. The malicious code will spawn 50 threads, each one dedicated to attacking a different host. The attack packets themselves will be randomized TCP syn packets and UDP packets of different size on destined for different ports, some containing text such as DIE_AMERICA. The attack will be timed to coincide with the physical terrorist event in the City. The net effect will be a paralyzing DDOS that will last at least 1 hour.

3. Destructive worm combines Slammer and Magistr Virus/Worm

A scanning worm exploits a vulnerability in MS_SQLbuffer overflow vulnerability. It will scan for other hosts listening on port 1433. After scanning for 10 minutes it will activate the malicious payload which will

- Erase CMOS on some hosts
- Erase the Flash BIOS on some hosts
- Overwrite every 25th file with the text "We Win-America Loses" as many times as it will fit in the file
- Delete every other file
- Overwrite a sector of the first hard disk

This will destroy the machines and require either factory reconditioning or new machines along with installing complete backups.

4. Anti-American sympathizers deface web pages

Due to world events, anti-American sympathizers work to sow confusion in two waves. The first wave will be attacks on actual web servers in the DMZ of the various domains. The second wave will be a DNS poisoning situation where web sites all over the country (including City, County, and State) will be re-directed to a domain at a university which will contain more anti-American propaganda.

5. Non-terrorist Criminal Forensic Activity

Various King County computers are noted by law enforcement as trying to break into a database holding credit card information. The computer is actually under control of a remote host, but the software to do its nefarious deeds was somehow installed on the computer. Law enforcement shows up and is asking about a computer which was logged on some time ago using DHCP and so the logs have to be consulted to go from DHCP address to MAC address and identify the specific computer. Sometimes the logs are on backup tapes. Sometimes they are gone because it is too long ago.

Seattle has a threatening e-mail to the President and the Attorney General. Dennis will construct header portion to give to USSS to use when they show up at the door. The header information will show that it came from a wireless device at

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

Seattle City and Light, and again, DHCP logs will have to be traced to find out the source, if they have been preserved long enough.

RIAA sends strong letters from their attorney to the Attorney General of the State threatening to take legal action if the State does not stop their employees from downloading MP3 files. This is directed at DIS, EMD, and DOT.

A federal law enforcement agent will go to each of the player cells to discuss these issues for about 30 minutes.

6. Logic bomb engages in cross-border game play (desktop Trojan)

An email containing a suspicious attachment and several web links will be sent to multiple recipients on every domain. The email will have news about a new security vulnerability, and recommend that the user download a patch or open the attachment. The attachment will contain a malicious payload that installs a timed logic bomb. The links appear to be to Microsoft, but they are redirected to a malicious gopher server will likewise infect anyone using Microsoft IE. The infected users will become unwitting attack agents for a timed DDOS against a domain in British Columbia. The attack target and time are hard-coded, but a machine in the City with a bad clock will start its attack hours too soon, tipping off a smart sys admin that the machine is infected. A local expert will be called in to look at the problem. After a memory dump and some code analysis, he or she will determine that the attack will take place in several hours, and realize that potentially hundreds or thousands of zombies are waiting for the appointed time. He will have to notify the appropriate American and Canadian officials to mitigate the attack. The attack will not actually occur as this problem chain is designed to exercise the various fan out procedures.

7. DHSS Threat level escalation from Yellow through Red

The exercise will begin at condition Yellow. The level will be raised to Orange by DHS when the possibility of a bio-terror event elsewhere in the country emerges. The players will be notified by the VNN news network (power point slides) or by email from "appropriate authorities".

The level will be raised from Orange to Red when the physical terrorist event occurs in the City. The offices of the County will be evacuated, including the County NOC.

Workers hear about it and log on to VNN to find out more. This loads the newtworks to some degree. Terrorists detonate a Radioactive Dispersal Device (RDD) in the flats area south of downtown. The wind is

~~For Official Use Only~~

TOPOFF2 CYBEREX – After Action Report

blowing north. As events unfold, the first responders determine there is radioactivity at the site, and are concerned over how much and how far it may have spread. The reason for the evacuation of county offices and not city offices is that different officials receive different inputs and also respond to the same inputs differently.

T2 AAR #041

Appendix B

Master Event Scenario Listing (MESL)

Vign.	Start	Inject Nature	Prob Chain	Injector	Stimulated
1	0:03	Port scans within expected range in daily report by County Net Admin	1	Network Admin-County	COUNTY
1	0:04	Router (CityLightR) to Seattle Public Utilities fails	1	Senior Network Controller	CITY
1	0:04	EMD e-mail server (StEMDEmail)dies	1	Senior Network Controller	STATE EMD
1	0:05	Router (County_TransitR) to King County Metro Transit fails	1	Senior Network Controller	COUNTY
1	0:05	EMD NetAdmin reports EMD e-mail server has died	1	Network Admin-State EMD	STATE EMD
1	0:05	Port scans within expected range in daily report by City Net Admin	1	Network Admin-City	CITY
1	0:06	City Police Dept writes e-mail complaining of loss of router	1	Help Desk	CITY
1	0:10	Port scans within expected range in daily report by EMD Net Admin	1	Network Admin-State EMD	STATE EMD
1	0:10	Port scans within expected range in daily report by DIS Net Admin	1	Network Admin-State DIS	STATE DIS
1	0:10	Port scans within expected range in daily report by DOT Net Admin	1	Network Admin-State DOT	STATE DOT
1	0:12	CERT sends e-mail about urgent Security patch - Microsoft Windows	5	CERT rep	STATE EMD
1	0:13	EMD help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	STATE EMD
1	0:14	CERT sends e-mail about urgent Security patch - Microsoft Windows, mentions relationship to past scanning activities	5	CERT rep	CITY
1	0:14	CERT sends e-mail about urgent Security patch - Microsoft Windows	5	CERT rep	STATE DOT
1	0:14	CERT sends e-mail about urgent Security patch - Microsoft Windows, mentions relationship to past scanning activities	5	CERT rep	COUNTY
1	0:15	DOT help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	STATE DOT
1	0:15	CERT sends e-mail about urgent Security patch - Microsoft Windows, mentions relationship to past scanning activities	5	CERT rep	STATE DIS
1	0:16	DIS help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	STATE DIS
1	0:17	King County help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	COUNTY
1	0:18	EMD e-mail server is restored	1	Senior Network Controller	STATE EMD
1	0:18	Seattle DoIT help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	CITY
1	0:19	EMD e-mail server is rebooted and seems to be fine. Don't know cause	1	Network Admin-State EMD	STATE EMD

1	0:21	County NetAdmin receives e-mail from Microsoft (without PGP signature) telling of urgent security update and directing people to web site to download the patch	12	Network Admin-County	COUNTY
1	0:22	Router to King County Metro Transit restored	1	Senior Network Controller	COUNTY
1	0:23	EMD NetAdmin receives e-mail from Microsoft (without PGP signature)telling of urgent security update and directing people to web site to download the patch	12	Network Admin-State EMD	STATE EMD
1	0:25	Router to SPU restored	1	Senior Network Controller	CITY
1	0:25	County Net Admin reports router plug had been knocked out, now restored	1	Network Admin-County	COUNTY
1	0:26	County Exec has received a media request about the loss of the Metro Transit Website and is concerned that county government networks are weak. Please prepare talking points for County Exex	1	County Executive's Office	COUNTY
1	0:27	Network Admin-router had been accidently unplugged, now restored	1	Senior Network Controller	City
1	0:30	Law enforcement officer comes over to talk about threatening e-mail written to President, e-mail header indicates source is the city network.	11	JTF Rep	CITY
1	0:33	DOT NetAdmin receives e-mail from Microsoft (without PGP signature) telling of urgent security update and directing people to web site to download the patch	12	Network Admin-State DOT	STATE DOT
1	0:34	load from outside internet directed at DOT server (StDot_Data) grows to 95%	1	Senior Network Controller	STATE DOT
1	0:34	e-mail servers (StateEmail) start to bog down with traffic	1	Senior Network Controller	STATE DIS
1	0:34	load from outside internet directed at EMD mail server (StEMDEmail) grows to 95%	1	Senior Network Controller	STATE EMD
1	0:35	help desk e-mails complaints of e-mails from various addresses with newspaper columns concerning war, taxes, environment, religion; some include links to web sites	1	Help Desk	STATE DIS
1	0:35	help desk e-mails complaints of excessive spam	1	Help Desk	STATE EMD
1	0:35	help desk e-mails complaints of excessive spam	1	Help Desk	STATE DOT
1	0:36	Secretary of Transportation has media inquiries about spam e-mail on DOT computers- PIO please respond	1	Secretary of Transportation	STATE DOT
1	0:40	e-mail from EMD Net admin advises of a malicious link-cross site scripting	12	Network Admin-State EMD	STATE EMD
1	0:40	e-mail from DIS Net admin advises of a malicious link-cross site scripting enclosed in e-mails and the possibility of compromised computers	12	Network Admin-State DIS	STATE DIS
1	0:40	Governor has received a call from media asking about Spam on State Accounts- please respond with talking points for Gov.	1	Governor's Office	STATE DIS
1	0:40	e-mail from DOT Net admin advises of a malicious link-cross site scripting	12	Network Admin-State DOT	STATE DOT
1	0:41	Governor has received a media inquiry about virus' in DIS e-mails. Please prepare talking points paper	12	Governor's Office	STATE DIS
1	0:54	load from outside internet drops back to normal due to installation of filters	1	Senior Network Controller	STATE EMD
1	0:56	County NetAdmin determines that the e-mail is not from Microsoft but is a hoax containing a Trojan	12	Network Admin-County	COUNTY
1	0:56	EMD NetAdmin determines that the e-mail is not from Microsoft but is a hoax containing a Trojan	12	Network Admin-State EMD	STATE EMD
1	0:56	DOT NetAdmin determines that the e-mail is not from Microsoft but is a hoax containing a Trojan	12	Network Admin-State DOT	STATE DOT

1	0:58	EMD NetAdmin writes expressing concern that upon reviewing the logs the same Trojan (Microsoft) e-mail has gone to most other users on the system	12	Network Admin-State EMD	STATE EMD
1	1:01	extra traffic on port 80 only from Far East (StEmdData), enough to show up on strip chart	5	Senior Network Controller	STATE EMD
1	1:01	a server (County_EmgData) in county seems to have a lot of load on it-not overloaded, but a lot	11	Senior Network Controller	COUNTY
1	1:01	FBI comes over to ask about a user who appears to be receiving personal data which could be used for identity theft	11	JTF Rep	COUNTY
1	1:01	extra traffic load all State DOT port 80 from Far East to (StDot_Data), enough to show up on strip chart	5	Senior Network Controller	STATE DOT
1	1:01	extra traffic to DIS on port 80 only from Far East (St_aceme_s), enough to show up on strip chart	5	Senior Network Controller	STATE DIS
1	1:02	Net admin reports a user has been receiving two e-mails per day, one with names, the other with bank account and social security numbers	11	Network Admin-State DOT	COUNTY
1	1:02	DIS Net Admin reports scanning traffic from Far East on port 80, but against non-web machines also - appears random	5	Network Admin-State DIS	STATE DIS
1	1:02	Port 80 scanning traffic noted in e-mail from EMD net-admin, showing up on non-web servers	5	Network Admin-State EMD	STATE EMD
1	1:03	extra scanning traffic on port 80 noted in e-mail from DOT net-admin, unique because it is also against non-web hosts	5	Network Admin-State DOT	STATE DOT
1	1:04	extra scanning traffic noted in e-mail from DOT net-admin	5	Network Admin-State DOT	STATE DOT
1	1:05	help desk e-mails complaints of excessive spam	1	Help Desk	COUNTY
1	1:10	e-mail from County Net admin advises of a malicious link-cross site scripting	1	Network Admin-County	COUNTY
1	1:15	traffic from Far East drops off partially	5	Senior Network Controller	STATE EMD
1	1:15	traffic on DIS from Far East drops off partially to 5%	5	Senior Network Controller	STATE DIS
1	1:15	traffic from Far East to DOT drops off partially to 15%	5	Senior Network Controller	STATE DOT
1	1:16	traffic from South America to DIS drops off completely	5	Senior Network Controller	STATE DIS
1	1:16	traffic from South America to DOT drops off completely	5	Senior Network Controller	STATE DOT
1	1:17	traffic from South America drops off completely	5	Senior Network Controller	STATE EMD
1	1:20	NIPC has notified State DIS via NASCIO only of extensive probing going on nationwide on port 80, may be related to earlier CERT advisory	5	DHS rep	STATE DIS
1	1:30	law enforcement comes and asks for disk image of computer serving MP3 files	11	JTF Rep	STATE DOT
1	1:31	DOT NetAdmin writes expressing concern that upon reviewing the logs the same Trojan (Microsoft) e-mail has gone to most other users on the system	12	Network Admin-State DOT	STATE DOT
1	1:32	City Police headquarters main line (City_Police_r) (City_r3) goes down and rolls over to a slower connection.	1	Senior Network Controller	CITY
1	1:32	Fire suppressant discharge in mainframe room at DIS	1	Network Admin-State DIS	STATE DIS
1	1:32	Loss of gateway router (StEmdR)	1	Senior Network Controller	STATE EMD
1	1:33	Loss of server (St_info_s) in mainframe room of DIS	1	Senior Network Controller	STATE DIS
1	1:33	EMD Communications line fails and automatic rollover to backup fails. (StEmdR) (St_client_)	1	Senior Network Controller	STATE EMD
1	1:33	USSS writes to say that a computer in county clerk's office has been attempting to crack into a personnel computer containing SSN's. They want to know which computer had a certain IP address 2 weeks ago. Police of slow response	11	JTF Rep	COUNTY

1	1:34	EMD reports loss of connectivity to their NOC, may be software problem	1	Network Admin-State EMD	STATE EMD
1	1:35	EMD reports that users are complaining they cannot get to the internet	1	Help Desk	STATE EMD
1	1:35	City Police hosts (City_Police_HQ)(Europe) generate heavy load as they are trying to download big files from somewhere	1	Senior Network Controller	CITY
1	1:35	help desk complains of users who cannot get out	1	Help Desk	STATE EMD
1	1:36	EMD Net Admin reports primary line is dead and secondary line did not activate - investigating	1	Network Admin-State EMD	STATE EMD
1	01:36	EMDNet Admin reports he just upgraded IOS before failure	1	Network Admin-State EMD	STATE EMD
1	01:37	City Help desk reports watch commander is really upset	1	Help Desk	CITY
1	01:38	Mayor has received an inquiry from the press saying the Police have lost access to their computer network. Please prepare a set of talking points for the Mayor	1	Mayor's Office	CITY
1	01:38	DIS Equipment failure (St_client_r) - rtr to DOT - coordinated event, not connected with fire suppressant	1	Senior Network Controller	STATE DIS
1	01:38	EMD Net Admin reports the router is fine, must be a telco problem on both lines	1	Network Admin-State EMD	STATE EMD
1	01:40	Equipment failure- rtr to DOT - no action required, done in DIS inject	1	Senior Network Controller	STATE DOT
1	01:40	City help desk reports police department noted utility workers in front of their building digging a trench	1	Help Desk	CITY
1	01:45	law enforcement comes and asks for disk image of computer serving MP3 files	11	JTF Rep	STATE EMD
1	01:45	Director of EMD has media inquiry about EMD being taken off-line by a hacker - please provide talking points	1	Director of EMD	STATE EMD
1	01:53	DIS Server returns to service	1	Senior Network Controller	STATE DIS
1	01:54	If required, EMD Net Admin reports he spoke with CISCO help desk and diagnosed problem	1	Network Admin-State EMD	STATE EMD
1	01:55	DOT Router returns to service	1	Senior Network Controller	STATE DIS
1	01:55	If EMD has not fixed problem by now,	1	Network Admin-State EMD	STATE EMD
1	01:56	DIS NetAdmin in control reports rtr to DOT unplugged by accident, now back in service	1	Network Admin-State DIS	STATE DIS
1	01:56	EMD Net Admin - if required- reports now on backup line	1	Network Admin-State EMD	STATE EMD
1	01:56	System back up and running normally	1	Senior Network Controller	STATE EMD
1	01:56	Note from DOT help desk that rtr was unplugged, now restored	1	Help Desk	STATE DOT
1	02:02	heavy load on host machine (St_HHSadm) (St_HHSs) in HHS	11	Senior Network Controller	STATE DIS
1	02:03	law enforcement comes and asks for disk image of computer serving MP3 files	11	JTF Rep	STATE DIS
1	02:03	County Communications line fails County_f1) (County_r4)	1	Senior Network Controller	COUNTY
1	02:04	load from outside internet directed at City mail server (CityEmail) grows to 95%	10	Senior Network Controller	CITY
1	02:05	help desk e-mails complaints of excessive spam	10	Help Desk	CITY
1	02:05	County Help desk reports failure in comms to outside world	1	Help Desk	COUNTY
1	02:05	Secretary of Transportation has media inquiries about a DOT employee using DOT computers to serve MP3 files. PIO please respond.	11	Secretary of Transportation	STATE DOT
1	02:07	County Net Admin reports primary line dead, secondary line works, but router not seeing it	1	Network Admin-County	COUNTY

1	02:09	County Net Admin reports router is fine, must be telco problem	1	Network Admin-County	COUNTY
1	02:10	e-mail from City Net admin advises of a malicious link-cross site scripting	10	Network Admin-City	CITY
1	02:10	Governor's office asks for a response to media about DIS employees operating MP3 servers on their computers.	11	Governor's Office	STATE DIS
1	02:22	If County has not requested by now, County Net Admin reports that router did not rollover to backup ISP automatically, he will take care of it	1	Network Admin-County	COUNTY
1	02:24	load from outside internet drops back to normal due to installation of filters	10	Senior Network Controller	CITY
1	02:25	County Net Admin reports that the rollover problem has been fixed and they are on backup	1	Network Admin-County	COUNTY
1	02:25	City Network admin sends e-mail that filters installed	10	Network Admin-City	CITY
2	00:01	Large amount of traffic out of Seattle City records host (inside of firewall). Causes server to waver between red and yellow and will not stop.	12	Senior Network Controller	CITY
2	00:02	netsim raises volume of internet traffic from internal County users to 80% to the outside US world as workers check news	13	Senior Network Controller	STATE DIS
2	00:02	netsim raises volume of internet traffic from internal City users to 80% to the outside US world as workers check news	13	Senior Network Controller	CITY
2	00:02	netsim raises volume of internet traffic from internal DOT users to 80% to the outside US world as workers check news	13	Senior Network Controller	STATE DOT
2	00:02	netsim raises volume of internet traffic from internal County users to 80% to the outside US world as workers check news	13	Senior Network Controller	COUNTY
2	00:02	netsim raises volume of internet traffic from internal EMD users to 80% to the outside US world as workers check news	13	Senior Network Controller	STATE EMD
2	00:03	Notice of threat change from NIPC per attached letter forwarded by NASCIO ISAC	13	Network Admin-State DIS	STATE DIS
2	00:04	EMD Users complaining that response on system is slow	13	Help Desk	STATE EMD
2	00:04	City Users complaining that response on system is slow	13	Help Desk	CITY
2	00:04	Help desk sends e-mail of complaints about response time	13	Help Desk	STATE DIS
2	00:04	DOT Users complaining that response on system is slow	13	Help Desk	STATE DOT
2	00:04	County Users complaining that response on system is slow	13	Help Desk	COUNTY
2	00:06	Traffic builds to 95%	13	Senior Network Controller	STATE DIS
2	00:06	EMD Users continue to complain system response is slow	13	Help Desk	STATE EMD
2	00:06	County Users continue to complain system response is slow	13	Help Desk	COUNTY
2	00:06	DOT Users continue to complain system response is slow	13	Help Desk	STATE DOT
2	00:06	City Users continue to complain system response is slow	13	Help Desk	CITY
2	00:07	NetAdmin of City reports that Cannot figure what is wrong with the bad host, and would like help procuring an outside expert. Don't want to just reinstall but analyze first. Can NOC find an expert?	12	Network Admin-City	CITY
2	00:07	Fish and Game complains poor response	13	Help Desk	STATE DIS

2	00:08	Help desk phones DIS to report many more complaints	13	Network Admin-State DIS	STATE DIS
2	00:08	County NetAdmin writes expressing concern that upon reviewing the logs the same Trojan (Microsoft) e-mail has gone to most other users on the system	12	Network Admin-County	COUNTY
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	STATE DIS
2	00:12	DIS Traffic drops down to normal 35-50%	13	Senior Network Controller	STATE DIS
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	STATE EMD
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	COUNTY
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	STATE DOT
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	CITY
2	00:14	DIS Help desk still reports complaints	13	Help Desk	STATE DIS
2	00:18	County Traffic drops down to normal 35-50%	13	Senior Network Controller	COUNTY
2	00:18	City Traffic drops down to normal 35-50%	13	Senior Network Controller	CITY
2	00:18	EMD Traffic drops down to normal 35-50%	13	Senior Network Controller	STATE EMD
2	00:18	DOT Traffic drops down to normal 35-50%	13	Senior Network Controller	STATE DOT
2	00:20	Governor's Office notifies all State department heads of change in Threat Condition to Orange	13	Governor's Office	STATE DIS
2	00:22	DOT Net Admin reports that they have shaped traffic to give lower priority to files of type .ra and .qt	1	Network Admin-State DOT	STATE DOT
2	00:22	City Net Admin reports that they have shaped traffic to give lower priority to files of type .ra and .qt	13	Network Admin-City	CITY
2	00:22	County Net Admin reports that they have shaped traffic to give lower priority to files of type .ra and .qt	1	Network Admin-County	COUNTY
2	00:24	County Help desk reports that public is writing and calling in to report several County websites are defaced with anti-American slogans	8	Help Desk	COUNTY
2	00:26	County Exec has received a media request about who is hacking the County websites. Please prepare talking points for the County Exec.	8	County Executive's Office	COUNTY
2	00:32	Governor's website defaced in call from Gov's Office	8	Help Desk	STATE DIS
2	00:33	DOT Help desk reports that public is writing and calling in to report several DOT websites are defaced with anti-American slogans	8	Help Desk	STATE DOT
2	00:33	City Help desk reports that a couple of primary web pages have been defaced with anti-American slogans	8	Help Desk	CITY
2	00:34	Labor & Industry website defaced reported in phone call	8	Help Desk	STATE DIS
2	00:34	EMD help desk reports that primary web page has been defaced (index.html)	8	Help Desk	STATE EMD
2	00:35	Mayor's office called, they have received a Media inquiry about web page defacements - please prepare talking points for the Mayor in 20 minutes	8	Mayor's Office	CITY
2	00:36	Governor's office asks for talking points to reply to media inquiry about defaced web sites	8	Governor's Office	STATE DIS
2	00:40	Director of EMD has media inquiry about website defacement - please provide talking points	8	Director of EMD	STATE EMD
2	00:53	DIS Net Admin gets really insulting e-mail from Darlene telling them to go to website and immediately download a system patch	1	Network Admin-State DIS	STATE DIS
2	00:57	DOT Net admin says all web sites are fixed	8	Network Admin-State DOT	STATE DOT
2	00:57	DIS Net admin says all web sites are fixed	8	Network Admin-State DIS	STATE DIS
2	00:57	EMD Net admin says all web sites are fixed	8	Network Admin-State EMD	STATE EMD
2	01:00	Secretary of Transportation has media inquiries about hacked DOT web sites, please provide talking points	8	Secretary of Transportation	STATE DOT

2	01:03	City NetAdmin receives e-mail from Microsoft (without PGP signature) telling of urgent security update and directing people to web site to download the patch	10	Network Admin-City	CITY
2	01:04	City traffic from a cluster to a single site on a computer off the internet grows to 85% of that site's capacity	10	Senior Network Controller	CITY
2	01:04	DIS help desk reports that a spoofed e-mail from (b)(6) is circulating in DIS	1	Help Desk	STATE DIS
2	01:05	DIS Help desk reports that the spoofed e-mail is popping up everywhere. Is it really her?	1	Help Desk	STATE DIS
2	01:09	Governor's office calls asking what is going on - media is asking about DIS employee who is spreading malicious software	1	Governor's Office	STATE DIS
2	01:15	City NetAdmin determines that the e-mail is not from Microsoft but is a hoax containing a Trojan	10	Network Admin-City	CITY
2	01:16	City NetAdmin writes expressing concern that upon reviewing the logs the same e-mail has gone to most other users on the system	10	Network Admin-City	CITY
2	01:22	Several Internal web servers on EMD network generate external traffic on port 80	5	Senior Network Controller	STATE EMD
2	01:22	Several Internal web servers on County network generate external traffic on port 80-saturate pipes	5	Senior Network Controller	COUNTY
2	01:23	Several Internal web servers on DOT network generate external traffic on port 80-saturate pipes	5	Senior Network Controller	STATE DOT
2	01:23	Several Internal web servers on City network generate external traffic on port 80	5	Senior Network Controller	CITY
2	01:24	State DOT help desk reports user complaints of getting out, internet is down.	5	Help Desk	STATE DOT
2	01:24	State EMD help desk reports user complaints of getting out, internet is down.	5	Help Desk	STATE EMD
2	01:24	City help desk reports user complaints of getting out, internet is down.	5	Help Desk	CITY
2	01:24	County help desk reports user complaints of getting out, internet is down.	5	Help Desk	COUNTY
2	01:25	Several Internal web servers on DIS network generate external traffic on port 80-saturate pipes	5	Senior Network Controller	STATE DIS
2	01:26	NetAdmin for City reports that the traffic coming from the web servers looks like port 80 web traffic destined for random addresses	5	Network Admin-City	CITY
2	01:27	State DIS help desk reports user complaints of getting out, internet is down.	5	Help Desk	STATE DIS
2	01:27	County Net admin says all web sites are fixed	8	Network Admin-County	COUNTY
2	01:30	All Internal web servers Scanning traffic drops abruptly from EMD networks	5	Senior NetworkController	STATE EMD
2	01:30	All Internal web servers Scanning traffic drops abruptly from City networks	5	Senior Network Controller	CITY
2	01:32	All Internal web servers Scanning traffic drops abruptly from DOT networks	5	Senior Network Controller	STATE DOT
2	01:33	All Internal web servers Scanning traffic drops abruptly on State DIS networks	5	Senior Network Controller	STATE DIS
2	01:34	All Internal web servers Scanning traffic drops abruptly from County networks	5	Senior Network Controller	COUNTY
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-State EMD	STATE EMD
2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	STATE EMD
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-County	CITY
2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	CITY

2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	COUNTY
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-State DOT	STATE DOT
2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	STATE DIS
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-City	COUNTY
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-State DIS	STATE DIS
2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	STATE DOT
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	STATE DIS
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	STATE DOT
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	CITY
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	COUNTY
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	STATE EMD
2	02:00	Outside scanning traffic on port 1433 stops.	6	Senior Network Controller	STATE DIS
2	02:00	Outside scanning traffic on port 1433 stops.	6	Senior Network Controller	CITY
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE DIS
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE EMD
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	COUNTY
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	COUNTY
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE EMD
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE DOT
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	CITY
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE DOT
2	02:03	EMD reports cannot retrieve data from contact database	6	Help Desk	STATE EMD
2	02:04	County help desk reports users complaining they cannot get to GIS data base	6	Help Desk	COUNTY
2	02:04	City help desk reports that electric utility reports they cannot get data from several databases	6	Help Desk	CITY
2	02:05	DIS help desk reports Health & Human Services Database is down	6	Help Desk	STATE DIS
2	02:05	DOT help desk reports that users complaining their data bases are not working	6	Help Desk	STATE DOT
2	02:07	County help desk reports users complaining they cannot retrieve data from their other data bases also	6	Help Desk	COUNTY
2	02:08	EMD help desk reports cannot retrieve data from Emergency Procedures database	6	Help Desk	STATE EMD
2	02:08	City help desk reports that water utility cannot retrieve data from customer database	6	Help Desk	CITY
2	02:08	DIS help desk reports State Police Database is down	6	Help Desk	STATE DIS
2	02:09	DOT help desk reports more users complaining data bases are completely non-functional	6	Help Desk	STATE DOT
2	02:10	Secretary of Transportation has media inquiries about loss of computer data bases. please provide talking points.	6	Secretary of Transportation	STATE DOT
2	02:10	Governor's office asks for talking points to reply to media inquiry about loss of state government databases	6	Governor's Office	STATE DIS
3	00:02	NetAdmin for DIS reports that NASCIO has forwarded a msg from NIPC to set Threat Condition RED	13	Network Admin-State DIS	STATE DIS

3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	CITY
3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	STATE EMD
3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	STATE DOT
3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	STATE DIS
3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	COUNTY
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	COUNTY
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	STATE DOT
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	STATE EMD
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	CITY
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	STATE DIS
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	Mayor's Office	CITY
3	00:06	help desk complains about slow response to users	13	Help Desk	STATE EMD
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	Governor's Office	STATE DIS
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	Secretary of Transportation	STATE DOT
3	00:06	help desk complains about slow response to users	13	Help Desk	CITY
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	County Executive's Office	COUNTY
3	00:06	help desk complains about slow response to users	13	Help Desk	COUNTY
3	00:06	help desk complains about slow response to users	13	Help Desk	STATE DOT
3	00:06	help desk complains about slow response to users	13	Help Desk	STATE DIS
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	Director of EMD	STATE EMD
3	00:10	Net Admin of DIS reports that they have just received a notification from NASCIO that says that DHS has declared condition RED due to a confirmed threat to the Pacific NorthWest in the next 24-48 hours.	13	Network Admin-State DIS	STATE DIS
3	00:10	NetAdmin of State EMD reports they have just received notification of an increase in threat condition from Orange to RED due to a confirmed threat to the Pacific NorthWest in the next 24-48 hours. Was received over the National Warning System (NAWAS) and National Law Enforcement Teletype (NLETS). The Governor, TAG and Director of EMD were also briefed by Secure VTC and STU-III in a conference call from Secretary Ridge, prior to the effective time in the change in level.	13	Network Admin-State EMD	STATE EMD
3	00:10	NetAdmin for City says that heavy traffic is coming from streaming video and suggests traffic shaping to fix it	13	Network Admin-City	CITY
3	00:12	Director of EMD has media inquiry about what their IT department actions are when they go to condition RED. Please provide talking points.	13	Director of EMD	STATE EMD
3	00:12	Governor's office asks for talking points to reply to media inquiry about what of threat level RED means for state computer systems	13	Governor's Office	STATE DIS
3	00:33	DDoS starts up against City networks traffic maxes out	5	Senior Network Controller	CITY

3	00:34	DDoS starts up against State DIS networks and maxes out	5	Senior Network Controller	STATE DIS
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	COUNTY
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	STATE EMD
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	CITY
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	STATE DOT
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	STATE DIS
3	00:35	DDoS starts up against State DOT networks and maxes out	5	Senior Network Controller	STATE DOT
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	COUNTY
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	STATE EMD
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	CITY
3	00:36	DDoS starts up against State EMD networks and maxes out	5	Senior Network Controller	STATE EMD
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	STATE DOT
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	STATE DIS
3	00:37	DDoS starts up against County networks and maxes out	5	Senior Network Controller	COUNTY
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	CITY
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	STATE DOT
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	COUNTY
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	STATE EMD
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	STATE DIS
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	CITY
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	STATE DOT
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	COUNTY
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	STATE DIS
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	STATE EMD
3	01:15	DDoS stops and network traffic drops to 90% from inside the city	5	Senior Network Controller	CITY
3	01:16	DDoS against State DIS stops	5	Senior Network Controller	STATE DIS
3	01:17	DDoS against State DOT stops	5	Senior Network Controller	STATE DOT
3	01:18	DDoS against State EMD stops	5	Senior Network Controller	STATE EMD
3	01:19	DDoS against County stops	5	Senior Network Controller	COUNTY
3	01:30	City is receiving complaints that the information on the city transportation web page is telling people to evacuate town	8	Help Desk	CITY

3	01:30	DOT Help desk reports that there is confusing information on their website about how to use all traffic lanes to leave town, no inbound traffic is allowed	8	Help Desk	STATE DOT
3	01:33	City NOC employees hear from friends that the County has been ordered to evacuate the NOC	13	Network Admin-City	CITY
3	01:34	We ask the County Executive to evacuate all the people from his NOC due to danger of radioactive plume, the ventilators for the building are still on and bldg mgme has evacuated.	13	County Executive's Office	COUNTY
3	01:45	DDoS starts up against City networks traffic maxes out	5	Senior NetworkController	CITY
3	01:46	DDoS starts up against State DIS networks and maxes out	5	Senior NetworkController	STATE DIS
3	01:47	DDoS starts up against State DOT networks and maxes out	5	Senior NetworkController	STATE DOT
3	01:48	DDoS starts up against State EMD networks and maxes out	5	Senior NetworkController	STATE EMD
3	01:49	DDoS starts up against County networks and maxes out	5	Senior NetworkController	COUNTY
3	02:05	Heavy DDoS on City's e-mail servers casuses them to quit.	1	Senior NetworkController	CITY
3	02:07	load on e-mail servers goes to 100% in a prolonged DDoS, preventing outgoing mail also	5	Senior NetworkController	STATE EMD
3	02:08	With the Email servers down, we are also having problems with out of band communications. Please discuss.	1	Admin Support & runners	STATE EMD
3	02:08	With the Email servers down, we are also having problems with out of band communications. Please discuss.	1	Admin Support & runners	CITY
3	02:10	Mayor asks City NOC how their staffing is to handle the workload	13	Mayor's Office	CITY
3	02:13	Employee in bldg calls to say that they cannot get an outside line, all phones are tied up - Need to call CISCO, and worried even if they get thru, CISCO might not be able to call back	13	Help Desk	STATE EMD
3	02:20	Governer calls to ask that DIS facilitate the recall of all essential governmental employees.	13	Governor's Office	STATE DIS

For Official Use Only

TOPOFF2 CYBEREX – After Action Report

APPENDIX C

SAMPLE SIMULATION COMMUNICATIONS OUTPUT

1218 20030506T13:46:34

To: netadmin.dot.control
From: dot.state.player
Subj: Email from city.player
Please apply filters to block that east coast domain.

20030506T14:53:49

To: netadmin.city.control
From: city.player@simserve1
Subj: Email from city.player
Please set egress filters at police_r to block everything other than 80, 8080 and 443 message

2991 20030507T13:58:50

To: dis.state.player
From: university.support
Subj: Email from dis.state.player Enabling such filters will greatly diminish the overall throughput of the routers as this will cause all packets to be process-switched through the router.

20030506T19:25:39

From :cert.support
From: city.player
How is the worm being propagated?

20030506T19:26:58

To: cert.support
From: county.player
Can you please provide us with any information on how to contact British Columbia Information Technology groups?

APPENDIX D

PRESS RELEASE

Gov. Locke Touts Success of TOPOFF2 Cyber Exercise

News Release - May 15, 2003 -- SEATTLE, Wash - - Governor Gary Locke announced the successful completion of the TOPOFF2 cyber exercise. The cyber exercise tested the response of the government's computer networks in the event it should experience a series of widespread, escalating cyber events.

The TOPOFF2 cyber exercise was part of the national TOPOFF2 exercise that began May 12 in Seattle and Chicago. The exercises featured sophisticated computer simulations, creating situations where state and local government information technology organizations had to respond in concert to a series of cyber security scenarios.

"This cyber exercise will help us be better prepared to respond to the possibility of disruptions or outages in our computer networks," Locke said. "I am proud of how our agencies performed and our ability to work across jurisdiction at the local, state and federal level."

Participants in the TOPOFF2 cyber exercise examined the actions required to limit potential damage caused by network compromise, and to minimize the impact on operations. The exercise required participants to make decisions in real-time in response to different, escalating events that slowed or stopped network operations. These events triggered management decision-making exercises about the associated business and communication functions required to recover the systems and resume providing essential public services.

"Working together in collaboration with the city of Seattle and King County, this exercise truly helped us organize a regional, coordinated response to a potential cyber event," said Stuart McKee, director of the state Department of Information Services. "The training was an excellent opportunity to test assumptions and effectively respond to a highly complex cyber incident."

Agencies involved in the cyber exercise included the state's Department of Information Services, Department of Transportation and Emergency Management Division, along with numerous agencies from the city of Seattle and King County, and the U.S. Department of Homeland Security, the U.S. Department of State, the local Joint Task Force of the FBI, the U.S. Secret Service and the U.S. Attorney's Office, as well as the private sector and Canada.

The TOPOFF2 cyber exercise is the first time an interactive, computerized network simulation has been used in public government, and was designed to create an "immersion experience" for participants. The Institute for Security Technology Studies (ISTS) at Dartmouth College created the network simulation.

This page intentionally left